Extending the User's Reach

Responsive Networking for Integrated Military Operations

David C. Gompert, Charles L. Barry, and Alf A. Andreassen

Center for Technology and National Security Policy

National Defense University

February 2006

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Extending the User's Reach. Responsive Networking for Integrated Military Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,300 5th Avenue,Washington,DC,20319-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**75**	

The views expressed in this article are those of the authors and do not reflect the official policy or position of The National Defense University, the Department of Defense, or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

David C. Gompert is a Distinguished Research Professor at the Center for Technology and National Security Policy, National Defense University. Prior to this position, he was the Senior Advisor for National Security and Defense at the Coalition Provisional Authority, Iraq. Mr. Gompert has held senior positions at the State Department, the National Security Council, the RAND Corporation, and in the information technology industry. He has published extensively on international affairs, national security policy, and information technology. Mr. Gompert holds a Master of Public Affairs degree from the Woodrow Wilson School, Princeton University, and a Bachelor of Science degree in engineering from the United States Naval Academy.

Charles Barry is a retired U.S. Army officer associated with National Defense University since 1993 as a military analyst specializing in transatlantic relations, defense information systems, U.S. grand strategy, and Army force structure. Mr. Barry has been qualified as a military strategist for more than 20 years and is considered an expert on strategy, international relations, and information systems related to command and control. He also consults on public-sector organizational development, productivity, and resource management. His current areas of concentration include DOD operational network integration, joint stabilization and reconstruction operations, and international capabilities in support of U.S. military operations. Mr. Barry is a doctoral candidate in Public Information Resource Management at the University of Baltimore.

Alf A. Andreassen is a Principal and co-founder of the Paladin Capital Group Homeland Security Fund, and serves as a member of the Boeing Corporation Homeland Security Senior Advisory Board. He has served on the Board of Advisors for the National Security Agency and on the Chief of Naval Operations Executive Panel. He has served on many corporate boards of directors, including as Chairman of Circadence Corporation, an information technology company; AgION Technologies, Inc., an antimicrobial solutions company, and PrivaComp, a medical information company. He has also served on numerous government-sponsored boards and task forces. Dr. Andreassen holds a Doctorate in Physical Chemistry from Cornell University and a postdoctoral fellowship in Materials Science.

Defense & Technology Papers ***are published by the National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available online at http://www.ndu.edu/ctnsp/publications.html.***

Contents

Executive Summary

The U.S. Department of Defense (DOD) is investing heavily in information systems to support net-centric military capabilities and joint operations. With such programs as Global Information Grid Bandwidth Expansion (GIG-BE), Transformational Satellite Communications Systems (TSAT), Joint Tactical Radio System (JTRS), and Net Centric Enterprise Services (NCES), DOD is creating a global information backbone and striving to get useful bandwidth and information services to the warfighter. After declining in the 1990s, spending on communications and intelligence has grown by 50 percent since 2001. Yet, the investment in networks still is not enough to harness the full power of information for national defense.

As long as it relies on current processes to design, fund, and acquire information systems, DOD will struggle to provide its users—joint warfighters—with the *access* to information and opportunities for *collaboration* that deeply integrated joint operations demand. In contrast to the primacy of users in creating information solutions in many sectors, and the Internet itself, DOD users are under-represented, under-privileged, and under-utilized in these processes.

At the same time, DOD cannot keep pace with and thus readily exploit powerful new information technologies that are propelled by larger, faster, and more fluid commercial markets. The protracted and inflexible ways DOD specifies its needs, allocates investment funds, and procures new systems are unsuitable for acquiring information solutions. This explains why DOD is a straggler in the use of Internet search technology and cellular communications, why customers within DOD increasingly bypass "the system," and why leading IT firms stay out of the defense market.

These anomalies will become more glaring and debilitating in the coming years:

- As demands grow for joint operational integration and, therefore, for information integration well below the Joint Task Force command level;
- As new technologies enabling users to seek and pull information from disparate networks flourish in the civilian world; and
- As adversaries start to exploit information infrastructure and networking principles with growing ease and speed.

The strategic danger is that integration of U.S. forces will be retarded and discredited by the failure of DOD to provide joint user-responsive C4 (command, control, communications, computing) solutions. Fixing this requires work at three levels: technology, processes, and governance.

The most momentous technology developments today are those that increase the power of networked end-users both in finding and using information and in shaping solutions, on the grounds that they know best what information and collaboration they need. The

new technologies that allow end-users to meet their needs and shape solutions are as important as distributed processing, the Internet, and mobile telecommunications, and they are changing whole industries for the better. The military potential of these technologies is especially great when considering the needs of war-fighters to pull relevant information from and collaborate across disparate networks and organizational boundaries.

With such user-reach technologies, the problem of network interoperability can be solved without wholesale replacement of the embedded base of disparate, non-joint systems. Connectivity standards can become user-responsive and largely self-enforcing. The need for and cost of systems integration can be reduced. And solutions can be continuously improved. If DOD is serious about the "user-pull" principle, it must catch this new wave.

Yet, DOD is at risk of having to swim after this wave, as it has swum after others. Its processes for setting C4 requirements, allocating resources to meet those requirements, and then acquiring capabilities are ponderous and insensitive to the needs of warfighting users in integrated operations. The separate military services, which dominate those processes, lack the perspective, ability, and incentive to meet joint C4 needs. Those who control money are network providers, not customers; and they do not put high priority on deeply integrated joint warfare.

The crux of these problems is that operational military users are bereft of market power. By giving control over resources to those responsible for joint warfighting and engaging them to fashion network solutions, DOD can shorten acquisition times, achieve information integration, and provide responsive systems.

For joint C4, the following changes are needed to shift power to users:[1]

- Requirements should be set by the joint warfighting community—in particular, Joint Forces Command (JFCOM), informed by needs of the Combatant Commanders (COCOMs). The Joint Capability Integration and Development System (JCIDS) is a step in the right direction but, as a bureaucratic planning process, it is inadequate.
- JFCOM should be responsible for seeking resources through the Defense Planning, Programming, Budgeting, and Execution (PPBE) system.
- JFCOM itself should acquire information solutions, relying on either Defense Information Systems Agency (DISA) or the military services as its procurement agents.

A new C4 acquisition process should be in harmony with the rapid and continuous way the IT market works and should seek to attract IT firms. This requires reform of the Federal Acquisition Regulation as it applies to joint C4, not work-arounds and waivers.

[1] By "joint C4," we mean IT solutions that are necessary to permit deep, joint, operational integration.

Revising and using new business processes for joint C4 will require purposeful governance. As strategic stakeholder, the Secretary of Defense (SECDEF) should articulate a vision and a standard:

- The vision is of deeply integrated and highly fluid joint operations.
- The standard is of unobstructed warfighter access to any relevant information and unbounded collaboration with any other warfighter.

SECDEF should also set the conditions for success by instituting process reforms and ensuring that adequate resources are devoted to user-responsive networks.

The Chief Information Officer (CIO) should answer to both the strategic demands of SECDEF and the operational demands of users. The CIO should participate in setting national defense strategy, ensure that reformed processes are functioning, measure progress, and provide network architecture and connectivity standards.

JFCOM should set, resource, and meet joint C4 needs. It should have the authority to interpret and act on COCOM needs. Such responsibility is in keeping with its basic mandate and should be its highest priority, given the criticality of C4 in joint operations.[2]

To support the CIO, JFCOM, and the rest of DOD, DISA should be the common technical resource, not only for global backbone support but also for connecting the warfighter.

Such an approach would lend solutions to a number of current issues:

- Existing efforts of each service to integrate networks in and across that service could and should be subordinated to and derived from joint C4 needs.[3]
- With users and the joint commands in the driver's seat, connectivity standards will be based on self-interest, not central policing, which is slow and ineffective.
- Legacy systems that are accessible by new technologies may be worth retaining even if they are not interoperable with one another.
- IT firms may be encouraged by process reform to enter the defense network solutions market, either directly or with defense contractors.
- Reconciliation of "user-pull" access and collaboration with "need-to-know" security concerns should be a challenge put to the IT industry.

In sum, if DOD aligns economic power with the joint community (the customer) in its processes; embraces the goals of deep integration, unobstructed access, and unbounded collaboration; draws the IT industry into its market; and elevates the role of the CIO, it can exploit the new user-responsive technologies and take a major leap forward in information integration, which is critical to a truly net-centric force.

[2] The roles of STRATCOM in global network operations would be unaffected. The Joint Staff (J-6) should support JFCOM and the CIO by ensuring that DOD processes are working as required.
[3] Service-specific information needs with no significant joint implications can be handled as usual.

Introduction

The aim of this study is to identify a path for the U.S. Department of Defense (DOD) to improve the responsiveness of military information networks for joint warfighters. This is not a technical treatise about bits and bandwidth; it proposes no architecture or standards. Rather, it looks at how military-operational information requirements relate to national strategy and at how those requirements are set and met. In particular, it considers how governance, economic power, and management processes within DOD should be aligned to maximize the prospects of meeting user needs.

This study relied principally on three methods to yield its findings:

- Review of important government documentation bearing on the use of information networking to support users in joint military operations.
- Interviews of persons from all the organizations involved in current efforts.
- Integration of strategic, military-operational, defense-institutional, technological, and economic perspectives and analysis.

Above all, this is an effort to widen the context in which defense networking is examined.

The chapters that follow tackle the subject in four steps:

- First, postulating a set of ideal general conditions under which DOD could match recent civilian-sector progress in meeting users' information needs.
- Then, analyzing current DOD efforts and plans to improve the responsiveness of military networks.
- Third, examining the promise of a new wave of IT that is propelled by user needs.
- Lastly, offering a concrete approach to removing the obstacles DOD faces in responding to warfighters needs and enabling joint integrated operations.

The logic, simply put, is to set ambitious goals without undue regard for the status quo, to understand conditions today, to learn from success in the larger world, and then to lay out a practical strategy.

The defense establishment is not the only organization that is concerned about user needs. After two decades of remarkable technological progress in the wider economy—from corporate data networking to the Internet to global infrastructure to cellular communications—attention has swung to how to satisfy the end user. Giving users the ability to summon whatever information they need, to collaborate with whomever they wish, and to shape information solutions to information needs is shaping up as the defining quest of this phase of the information revolution. Just as DOD has been a beneficiary of other major waves, it can gain immensely from this one.

But DOD is a notorious straggler in exploiting IT, owing to bureaucratic processes, parochialisms, and mega-programs that clog the channel between IT users and creators. The expanding information demands of the warfighter and the strategic imperative of deeply integrated operations argue strongly for making whatever reforms are needed to clear that channel and extend the reach of users into the limitless world of information.

This study was done with the support of the Office of Force Transformation in the Office of the Secretary of Defense. It profited from the openness and insights of many people and organizations inside and outside of DOD—few of which defended the status quo.

I. The Ideal: Integrated Information for Integrated Operations

Putting the User First

The truest measure of any information network's value is how well it meets the needs of its users, particularly the ease with which they can collaborate over it and the timeliness and richness of the information to which it gives them access. By this simple standard of user-satisfaction, the Nation's defense networks, including those that support military operations, have a distance to go. Moreover, with IT becoming increasingly user-driven and user-responsive in the wider civilian world, and with the rising hunger for information among warfighters in integrated operations, there is a risk that DOD will fail to "catch the wave" just when its own users—the troops—and the Nation need it.

At present, U.S. forces operating jointly make do with a mishmash of networks that neither satisfies warfighter needs for prompt and abundant information nor permits them to team easily across service lines. Operationally and tactically, this limits their abilities to make well-informed decisions and to collaborate spontaneously in the face of sudden battlefield challenges and opportunities. Strategically, it denies the full promise of integrated operations that can give U.S. forces decisive advantages.

Most extant command, control, communications, and computing (C4) networks[4] and other defense information systems were built for specific service, branch, agency, or other parochial needs. They were not designed to support integrated joint operations, to communicate with one another, or to be components of a larger network of networks. Even now, new systems are being designed and procured by the separate services, with uneven degrees of attention to how well they will advance the awareness and collaboration of users in integrated joint operations. Thankfully, this problem of networks that are unresponsive to the needs of warfighters in integrated operations is clear to DOD's leadership, which is now struggling with how to overcome it.

Unresponsive military information systems are antithetical to what is expected of the new joint warfighter in the new operational environment.[5] At every level and regardless of armed service, fighting units and those who lead them are supposed to act with unparalleled speed, creativity, flexibility, precision, and knowledge. They need to learn in the field, on the move and under fire, to refine decisions as they learn, and to support and rely on fellow units and sister services. In the confusion and urgency of contemporary

[4] We use the expressions C4, battle management, and joint operational networks more or less interchangeably, although experts like to make distinctions among them. Additionally, we use C4 rather than C4I or C4ISR or C4ISTAR (command, control, communications, computing, intelligence, surveillance, target acquisition, and reconnaissance) because C4 captures our intended meaning and because we are not directly concerned with sensors.

[5] By using the terms *warfighter* and *warfighting*, we do not mean to imply that responsive and accessible networks are relevant only to war. Most, if not all, possible military contingencies pose equally compelling demands on information networks.

war, as well as the ambiguities of operations short of war, warfighters are expected to use all relevant information to augment their intuition and quicken their reasoning as they make critical decisions.[6] They are expected to "self-synchronize" and "self-organize," revising plans and forming ad hoc cross-service teams in action. This is a tall order, not only for warfighters, but also for the networks that are supposed to inform and link them.

The current era, in Defense Secretary Rumsfeld's words, is one of "strategic uncertainty" regarding future global security conditions and thus the requirements of U.S. national defense.[7] All the more reason to tap as effectively as possible into the continuing revolution in information technology, especially as it informs and connects humans to tackle uncertainty in their many endeavors. Networked warfighters able to conduct integrated operations will be of great importance no matter what challenges the future holds, and as challenges shift without warning.

If global terrorist webs like al Qaeda remain the principal threat, the availability of timely information from all intelligence sources and the ability of forces to collaborate, regardless of service or agency will be crucial in tracking and striking the killers before they slip away. At the other extreme, if a technologically sophisticated and well-resourced challenger emerges in a region of vital concern—say, China in East Asia—the shared awareness and joint integration of U.S. forces will be increasingly critical to offset their potential vulnerability to long-range enemy sensors and weapons. In any plausible future, national defense demands networks that give U.S. soldiers information superiority and the ability to collaborate as circumstances require.

Ideally, any joint warfighter should be able to pull data from any source or sensor, to communicate and collaborate with any capability resident in the force, and to function within any C4 system. At present, U.S. armed forces are busily crafting joint operating concepts on the assumption that user-responsive, jointly-accessible networking is at hand. Absent such information integration, these dependent investments are at risk, as is the goal of operational integration. Network inadequacies alone can stall transformation.

In theory, these needs will be addressed by DOD via the creation of new joint information systems that will over time form a sort of union of networks optimized for integrated operations, replacing the existing welter of networks. Systems designed expressly to provide C4 for joint warfare and to support new operating concepts should help satisfy user needs for both access and collaboration. But there is plenty of room for spillage between cup and lip with such a strategy—poorly communicated user needs, a ponderous if not inimical acquisition process, lack of IT breadth and depth among defense contractors, insufficient motivation among the separate armed services, lack of interest in defense on the part of leading IT firms, and inadequate standards, to name some. Meanwhile, the separate armed services are investing in information networks to

[6] David Gompert, Irving Lachow, and Justin Perkins, "Battle-Wise: Gaining Cognitive Advantage in Networked Warfare," *Defense & Technology Paper* 8, (Washington, DC: Center for Technology and National Security Policy, January 2005).
[7] *The National Defense Strategy of the United States of America*, 2004.

satisfy near-term operating demands and to improve integration within each service, the contribution of which to joint integration is at best unclear.

DOD does not presently satisfy the dynamic organizational and economic conditions that give vitality to the information revolution and energize the growth of user-responsive networks in the world at large. Simply to blame this on bureaucracy ignores the point that incentives, means, and goal are misaligned in DOD when it comes to information integration. Those with the greatest stake in the goal lack the means (i.e., dollars) and authority to affect it, while those with means and authority have priorities they consider higher than the goal. For the organizations that command and dispose of defense funds—the separate armed services and acquisition authorities—there is insufficient return to justify the investment cost of replacing otherwise serviceable non-joint C4 systems before they age out. Because the services are not responsible for operations, they do not necessarily feel the urgency of incorporating the latest IT innovations. Because the services are not held responsible for achieving joint integration, they tend to see joint C4 as a thin appliqué to service-based C4—more relevant to the joint force commander than to the soldier, sailor and airman (as if civilian business-to-business - B2B - connectivity were only worth having at the board of directors level.) Although the current service chiefs have justly earned a reputation for joint-mindedness, such luck in personal qualities cannot be counted on to overcome the institutional biases of the services.

Since truly integrated joint warfighting is in its infancy, the inadequacy of service-based C4 systems has yet to be fully experienced or perceived. No wars have been lost because joint forces cannot pull all the data they need or collaborate readily with one another. Moreover, in peacetime, when most investment decisions are taken, user (i.e., joint warfighting) organizations are essentially shells. As a result, there is no institutional ground-swell of demand for "integration now."

Although there is no sense of crisis, there are indicators of trouble to come. For instance, ragged air-ground C4 and collaboration during Afghanistan's Operation *Anaconda* turned what should have been a "simple" joint operation into a crisis.[8] Urban combat operations are plagued by the inability of scattered U.S. forces to share data with one another. During Operation *Iraqi Freedom*, while headquarters had bountiful, fused information, warfighters on the move went hungry for bandwidth.[9] In subsequent counter-insurgency operations in Iraq, latency in information about the identity, location and activities of insurgents and terrorists has kept U.S. and Iraqi forces from arriving before the enemy has vanished. The cacophony of demands of regional combatant commanders (COCOMs) for more responsive information systems for deployed and deploying units suggests that DOD business processes are not able to respond to the needs of joint warfare.

[8] Richard Kugler, Michael Baranick, Hans Binnendijk, "Anaconda's Lessons for Joint Operations," to be published as a *Defense & Technology Paper* by the Center for Technology and National Security Policy, National Defense University.

[9] Maryann Lawlor, "Iraqi Communications Transition From Tactical to Practical: Military builds Foundation for the Future," *SIGNAL Magazine*, November 2004.

On the face of it, current approaches to supporting warfighter information needs appear to be inadequate for this formative stage of both force transformation and networking. Tinkering with these approaches almost certainly will prove inadequate. Joint operational integration is needed as soon as possible. It is potentially a huge and crucial U.S. edge. Afghanistan, Iraq, al Qaeda, and growing Chinese offensive capabilities suggest that the new global security environment already demands it. Yet, lack of jointly accessible and responsive networks will retard if not abort the effort to overhaul operating concepts and gain the benefits of integration. The lack of information integration could discredit operational integration and reinforce old habits of service-by-service self-reliance in plans, capabilities and action. In a vicious spiral of sinking expectations, lack of connectivity could cause U.S. forces and DOD to lower their sights on integration and transformation to the point that user-responsive networks will not seem imperative after all.

Alternatively, warfighters with unmet demands for information access and collaboration might be seduced by the siren call of the Internet. After all, the essence of the Internet, and what accounts for its extraordinary growth and development, is its user-responsiveness. The military *should* exploit Internet technologies, the Internet itself, and other public utilities to help meet its information access and collaboration needs. Still, many public systems lack the security the military needs precisely because they are meant to maximize access. And security can make the difference between victory and defeat in war. The Internet is inexorably drawn toward universal access, ease of use, and ease of interconnection, making all who use it potentially vulnerable to those who would misuse it. After all, use of the Internet is something that al Qaeda and the U.S. forces that stalk them have in common. Nor can the Internet provide adequate tools for the uniquely violent, urgent, and vital circumstances of warfare. The leader of an ambushed unit cannot be browsing for information to clarify circumstances and options.

Defense network deficiencies are rooted as much in governance and business processes as in architecture and technology. Control over the capabilities of information systems and services remains largely in the hands of those who provide them: the separate services, functional organizations, the technical establishment, acquisition authorities, and defense systems vendors. Like “Ma Bell” of old, today’s defense network providers define needs and set budgets and timetables to meet them—an economically upside-down condition that discourages innovation and impedes progress.[10] In that model, networks belong to those who furnish them rather than to those who use them. (Again, the sharp contrast between Ma Bell’s network and your Internet is instructive.) Users—unified combatant commands, other joint commands, and joint warfighting forces—have had little say. Except for urgent needs, such as those associated with an impending deployment, users have been effectively locked out of the process of determining requirements and locked into the results.

[10] The analogy is not a casual one. Before being broken up, the Bell System set network requirements and performed research, development, and network engineering to meet them at its own speed and economic logic. After the break-up, competition and the emergence of user-power opened the way to what we know as the Information Revolution and eventually the Internet.

The traditional force-planning process, even with its recently increased attention to joint requirements, cannot adequately communicate user needs, taking too long and weakening demand signals. Even DOD's civilian leaders have little practical leverage to ensure users' needs are met—essentially, a bully pulpit and stewardship of an unenforceable unifying architecture. Lacking market power, those who see the imperative of user-driven C4 solutions are condemned to live with what is furnished them by those who do not necessarily share their joint-operational vantage point or their sense of urgency.

In truth, when it comes to meeting users' information needs today, the situation is not so grim. U.S. forces are certainly not crippled by limited awareness and collaboration. However, the promise of joint operations and the growing reliance on information will soon open a gap between what is needed and what is possible. DOD efforts to meet joint warfighter needs must be sufficient to avoid this.

Experience in the Wider World of Information Networks

If current networks are not adequate to support the growing information and collaboration requirements of joint users, neither do they fit the prevailing model of non-military information systems, networks and services in recent years—defined by users, demanded of providers, and consequentially open and responsive. Indeed, the principal reason that distributed computing, data networking, and the Internet have expanded and contributed as much as they have is the primacy and insatiability of the networked user (by which we mean end user, not IT purchasing manager). Networks, user-dominance, and connectivity make a potent cocktail, but only when all exist. Of course, the military recognizes this and has embraced the Internet Protocol (IP) as the basis for information networking—a necessary but by no means sufficient measure to catching the user-reach wave.

DOD and the joint warfighting community are far from the first institutions to find their paths blocked by unresponsiveness networks and providers. Before users demanded open architectures and standards, proprietary computing systems and poor network connectivity were commonplace—part and parcel of vendors' business strategies (i.e., customer lock-in and "account control"). Complicit in these strategies were management information systems (MIS) departments whose lives were made simpler by having, and accommodating, a dominant vendor. As technology progressed—above all, the merging of computing and communication into data networking—the proprietary- provider-dominant structure threatened to stunt the exploitation of distributed processing and thus collaboration throughout the enterprise. It also blocked the rise of inter-company and economy-wide networks. The real information revolution would have been still-born, and the Internet never more than a gleam in the eye, had this structure not been demolished.

As we know, users prevailed, and remarkable progress followed. In many sectors—notably, financial services, manufacturing, retail, and transportation—the demand of large, economically powerful business users for connectivity among and greater value from information systems led the way. Corporate leaders and users came to see closed systems as unresponsive to their operations and strategies. They wanted pathways into the information era and faced dead ends instead. So they turned on, and often tuned out,

those who would foreclose their options and retard networking. Vendors and systems integrators had to improve responsiveness and design for connectivity or lose share. The network train left the station, with the user driving the locomotive.

Several inter-related conditions contributed to this development:

- The availability of open operating systems and architectures, starting with UNIX, an operating system (which was, incidentally, invented by users who wanted to work together).[11]
- The appeal of networking as a natural and productive way for people to work—in horizontal collaboration—leading to demands for connectivity and rewarding the vendors that delivered it.
- The growing business significance of information and information systems, and thus the awareness of top management that the interests of external customers and internal users must dictate requirements.
- The eclipse of the mainframe and mini-computer markets by the explosion of distributed desk-top processing, which demanded connectivity.
- Associations of users with a common interest in and insistence on standards, creating market power which vendors could not but heed.

Resultant market forces produced a rush to openness, making proprietary systems not merely unpopular but obsolescent. All but the most obtuse computer vendors saw the train leaving and got on—though some have found themselves in the caboose.

With the advent of openness, a new corporate IT governance model appeared. The replacement of the MIS department head by the Chief Information Officer (CIO) in many corporations both reflected and facilitated these market-technology dynamics. The position of CIO is meant to promote the business side of the enterprise: the internal user (revenue and profit-margin), the external user (customer satisfaction and price), and the shareholder (assets and earnings). The chief constituents of the CIO are the line operating units, which depend vitally on access to responsive, corporate-wide information networks. Additionally, because Chief Executive Officers (CEO), Chief Operations Officers (COOs), Chief Financial Officers (CFOs), and boards of directors now understand the critical role, considerable investment costs, and productivity potential of information networks, they view them in relation to profitability and corporate strategy, and they therefore want a senior corporate officer looking after their acquisition and use. With the decline of proprietary architectures, the CIO can extract maximum value from and incite fierce competition among vendors (the opposite of the instinct of the old MIS). In turn, the CIO answers to the users as well as to the CEO and board.

While some lessons from the revolution in IT governance and connectivity can be learned from corporate experience, it will be hard to replicate in DOD the market forces, income motivations, and profit metrics that have placed corporate users, leaders and shareholders in control and chased out proprietary systems. Even so, the CIO can be the agent of openness, standards, user dominance, and strategic responsiveness in DOD, answering to

[11] UNIX was created by Bell Labs researchers for their own use.

both the CEO (the Secretary of Defense) and the line operating units (the combatant commands). But is must be understood that a CIO's mission, in DOD or elsewhere, will be quixotic if larger business systems are not reformed insofar as they relate to IT.

There are also sectors, such as health services, with persistent information network problems like those faced by the military, for some of the same conditions of fragmented governance, parochialism, and administrative encumbrance that plague DOD. Information users—namely doctors and patients—have been weak "market players." Hospital bureaucracies, departmental stovepipes, and IT vendors have had little incentive to provide networks designed for user access and collaboration. Yet this is beginning to change. We will share in Chapter 3 a promising effort to give doctors ready access to the archipelago of data islands where treasured information is buried.

In other sectors—air travel, for instance—the Internet has enabled customers to seize control, bypassing airline information systems, squeezing middlemen, sending fares down, rewarding low-cost carriers, adding to competitive pressure on entrenched carriers, and stimulating creation of more responsive information systems. Notwithstanding the differences between defense and other sectors, management, economic and technological lessons for DOD can be learned from methods and reforms being attempted in sectors that have mastered, or are still struggling with, user responsive information integration. Above all, a user coup is needed.

Criteria, Metrics, Responsibilities and Economics

The defense establishment lacks the financial motives and measures by which commercial enterprise is able to set, track and score the operating contributions of information systems and services. Cost-effectiveness is a poor proxy for profitability, and even cost-effectiveness is hard to gauge when it comes to C4 networks. It is possible to measure and compare costs of designing, building and operating networks; but quantifying network effectiveness—the contribution to the outcome of battle—is largely guesswork, especially in the case of C4 systems, what with intangible cognitive and subjective factors at play that are hard to model.[12]

The point is not that the United States is failing to invest enough in communications and intelligence for U.S. forces. Total C4ISR budget for defense has jumped from $35B in 2001 to $54B in 2005, following a gradual decline during the 1990s; and it is now 14% of the total defense budget, compared to about 10% in the 1990s.[13] Whether this is enough is beyond the purpose and scope of this study. Much of this is for investment in sensors and in new infrastructure—e.g., the Global Information Grid (GIG)—needed to provide ample bandwidth to U.S. forces in the field around the world. While this investment will continue, the greater challenge now is to fashion information solutions that help

[12] Research has expanded recently into understanding the cognitive aspects of C4. Despite some progress, it is still difficult to model or show quantitatively what difference it makes to give warfighters improved access to information or to enable them to collaborate. In effect, it is hard to prove, much less to measure, the benefit of open systems relative to their cost and to other systems.

[13] Numbers are in constant 2004 dollars.

warfighters at every level meet the operational challenges they face in the unfamiliar, fluid, and unpredictable new security environment. For planning purposes, the infrastructure can be regarded as largely "given," and further investment should be guided by the needs of users—*defined by users*—for awareness and collaboration in joint operations.

The absence of financial motives and measures to guide network development is both a macro and micro problem for DOD. How can one weigh the value of the ability to conduct unconstrained joint operations against the billions it would cost to create a fully integrated and responsive union of networks? How can new investment in jointly accessible systems, or in technology that can pry open closed systems, be compared to the more direct and measurable contribution of this or that new weapon or platform or sensor competing for the same funds? When there is no price mechanism, how can users signal the strength of their preference for responsive information systems and features? When there is no way of calculating rate of return, how can investment in such capabilities be rationally apportioned?

Commendably, the Defense Department has reformed its force-planning process in recent years to ensure that joint concepts of operation can be supported by capabilities.[14] As analysis performed by the Joint Staff identifies investment opportunities to advance integration, a committee consisting of the Vice Chiefs of Staff of the military services reviews and may endorse them, thus mandating service compliance.[15] However, staff analysis and four-star intervention cannot substitute for setting and communicating requirements by users with funding power. A process that counts on a huddle of flag officers from different services to transcend service boundaries will, at best, produce slow and bumpy progress where major, continuous, and urgent results are needed. The world has learned that central planning is no substitute for markets.

Of course, the defense establishment is not and cannot be a true market. Lacking profit motives and measures, the best DOD can do is set criteria that link information network responsiveness to strategic and operational goals; devise metrics that mark the degree of satisfaction of these criteria; and align economic power with user demand.

Criteria must start at the strategic level and cascade from there. Strategically, information networks must permit U.S. forces to meet the full spectrum of national security needs and international security interests and responsibilities of the United States at acceptable levels of casualties and cost. To this end, networks must give U.S. forces operating jointly sufficient awareness and opportunity for collaboration to provide them with decisive advantages—e.g., speed, mobility, dispersion, survivability, precision, lethality, and cognitive acuity—over opposing forces. This further implies that warfighting units, regardless of level, must be able to get instant access to any information that could help

[14] The Joint Capability Integration and Development System (JCIDS) is the system the Army uses to identify its capability needs.
[15] The Joint Requirements Oversight Council (JROC) is the principle forum in which senior military leaders address requirements from a joint perspective.

them perform and to connect without delay or interference with any unit that may be of assistance.

From these criteria, metrics could be developed. Again, in the ideal, any unit must be able to collaborate with any other unit and have access to information from any source throughout the force. Although this is a distant vision, the extent to which it is realized—as measured by technical means, exercises, operations, and impartial analysis—would suggest how much progress has been made and how much has yet to be made, as well as where the blockages are.[16] In line with such reasoning, more specific criteria could be developed regarding key operational challenges, e.g., the ability to conduct fully integrated air-ground maneuver operations with or without local basing; to establish air control over defended hostile territory; to eliminate deployed weapons of mass destruction; to create an expandable land lodgment anywhere; to crush terrorist or insurgent pockets without collateral damage in cities.

Because DOD is not a true market, there is no invisible hand to guide its choices. Because it has no invisible hand, it must be clear who is responsible for satisfying information integration criteria. The Secretary of Defense is ultimately responsible for satisfying the strategic criteria for network adequacy—namely, joint integration and the accompanying *any-from-any* access and *any-with-any* collaboration standards. Combatant commands, assisted by other joint commands, are responsible for satisfying the criteria associated with key operational challenges.[17] In both cases, progress or the lack thereof can and should be measured. The CIO should be responsible for ensuring that DOD processes support both the leader (Secretary) and users (joint commands) in the realization of progress toward the strategic and operational criteria, respectively. This requires translating criteria into network functionality, connectivity, architecture, standards, and systems priorities. These expectations fall within an even wider definition of CIO responsibilities encompassing the "business" side of defense along with the operational, namely, to create conditions for adequate information flow at all levels.

In sum, having an articulated ambition, however distant and ideal, would both provide motivation and permit measurement. Because the status quo is known and because the ambition can be translated into operational and technical terms, it should be possible to measure the distance between them, progress over time, deficiencies, information network performance requirements, and the contribution of investments, whether in new systems or in opening up extant systems.

Providers—services, acquisition authorities, R&D labs, defense contractors, and IT firms—need not be subject to such criteria and metrics. Indeed, they should not, for this would only confuse the issue of where responsibility lies, i.e., with leaders (the Secretary), users (COCOMs), and the CIO. The job of providers is straightforward: to satisfy corporate and user information-network criteria, as endorsed by the CIO. If they

[16] The ideal stated here is not far-fetched when considering that the Internet meets this standard.
[17] Holding combatant and other joint commands responsible for measurable progress against such standards is desirable in any case. While essential in generating information network requirements, this would also help in generating or at least checking other capabilities (e.g., weapons) requirements.

do not, what they offer should be rejected—indeed, *would* be rejected—by users intent on meeting their criteria and discharging their responsibilities. Information systems that do not provide connectivity for joint operations will fare badly in competition with those that do. In other words, internal providers, like external ones, should have to gain user acceptance.

The basic arrangement just described will not work unless users are able to back what they demand with something that moves providers—money. Economies do not work when "demand" has no economic meaning, as is the case for IT within DOD today. This requires finding a way of giving users control over investment funding for information solutions relevant to their criteria.[18] We will return to the questions of how requirements are set, how funds are allocated, and how investments are chosen and managed; however, our bias is to shift power over these functions in the direction of users.

Using funding power to back demand would be relatively straightforward (if bureaucratically disruptive) for procuring new joint C4 networks. But what of the large overhang of existing service-based and proprietary legacy systems? There is merit in measuring the extent to which existing systems satisfy corporate-strategic and user-operational needs. Therefore, existing systems should be held up to exactly the same criteria as new ones. This would permit a rational apportionment of investment resources among the alternatives of replacing existing systems with joint-by-design systems, remedying their deficiencies (e.g., mitigating their lack of connectivity), and just letting them be if they do not affect joint operations.

Thus, the leader must meet the national strategic criterion of creating the ability to conduct integrated joint operations; joint users must meet key operational criteria; the CIO must translate the leader's and users criteria into network requirements; internal providers (mainly the services) must offer solutions that satisfy these criteria. If funding follows this logic, the laws of economics should flow resources toward those investment options that return the most to user access, collaboration, and integrated joint operations.

Criteria, Metrics, Responsibilities and Economics (Continued)

Chapter 2 will describe and analyze current DOD conditions that affect the prospects for satisfying these criteria and, thus, the vision of information integration. Before examining "ground truth," which will of course influence the proposals to come at the end of this volume, it is useful to lay out a *general model* for achieving and sustaining information integration. To the extent that current conditions are close to the model, proposed changes can be modest. Conversely, the extent to which current conditions fall short of the model should determine the strength of the medicine to be prescribed.

[18] Again, the Ma Bell analogy is instructive. Because its profits were set and controlled by regulation, the AT&T of old did not place much weight on user demand in deciding how much to invest in what network enhancements.

Our frame of reference for considering the model is:

- that the interests, responsibilities and military strategy of the United States in this complex and fluid security environment demand an ability to conduct increasingly integrated, flexible and speedy joint operations;
- that such operations demand network solutions that responds to two basic information needs of joint war-fighters: unhindered access to information and easy communications among collaborating units;
- that a rational system of criteria, metrics, responsibilities, and alignment of funding power with user-demand must substitute within DOD for the market forces that have delivered connectivity and improved user-responsiveness in the civilian world of information.

With information integration the goal, it follows that networks, unless dedicated to clearly and wholly single-service needs, must be either joint by design or otherwise rendered accessible to any and all forces operating jointly. In the long term—when, as Keynes observed, we are all dead—attrition of extant systems and fielding of joint ones would get the U.S. military to the goal. However, given today's difficult international security environment, waiting a decade or more before integrated operations are made possible by a unified and responsive network is unacceptable. At the same time, the costs of wholesale replacement of existing systems would be prohibitive, given today's tight fiscal situation. Therefore, if there are feasible and affordable ways of making existing systems accessible and responsive—a crucial "if"—a draconian network-replacement campaign makes no economic sense.

Ideally, DOD can make significant and reasonably quick progress through a combination of fielding new joint systems and enabling old non-joint ones, within a common architecture and with the expansion of the new gradually superseding the old. The pace of replacing existing networks with joint ones depends on the cost and efficacy of technological options to enable the existing ones to support integrated joint operations. Fortunately, technologies that allow access to disparate existing systems and technologies that are the basis for new joint ones are likely to converge around the new wave of user-reach solutions (to which we will return in Chapter 3).

In order to exploit these technologies both to build new systems and to enable old systems in response to the demands of integrated joint operations, DOD will need a set of guiding principles and a reformed system of governance, responsibilities, and economics. The principles and the reformed system must strengthen the hand of users and yet fit within the broad contours of the way government and the military establishment function—that is to say, consistent with the tenets of fair, competitive procurement and sound, transparent management of public monies.

We know from non-defense experience that information integration cannot be achieved by the fiat of some governing authority. (In the commercial universe, the most consequential act of government was a negative one: withdrawing state protection from telecommunications monopolies and thus removing an obstacle to new technologies,

applications, and markets.) At the same time, by establishing key principles, leadership can set goals, conditions and general direction. We suggest these:

- First, the national security interest in effective joint operations of networked forces will be the ultimate standard, not only for new systems but extant ones. As the strategic standard-bearer, the Secretary of Defense will be judged accordingly.
- Second, requirements will be determined by, and thus should not constrain, critical joint operating concepts. Under strategic guidance, these will be developed by users (joint commands), who will be responsible for meeting them and measured accordingly.
- Third, existing information systems relevant to joint operations will not be grandfathered but instead held to the same strategic and operational criteria, expectation of user-responsiveness, and standards. If they do not make the grade, they must be enabled, if economically feasible, or else they must be abandoned.
- Fourth, users will have the means and authority to buy joint C4 networks or enhancements that address their needs for information and collaboration.
- Fifth, providers are expected to satisfy these requirements and user needs; solutions that are not responsive to joint warfighters may be rejected by users in favor of those that are. Competition is welcome.

These should serve as the five commandments for DOD's CIO. Answering both to the strategic stakeholder (the Secretary) and to line-operating units (COCOMs), the CIO should be judged by how well strategic and operational criteria for information networks are being met. More specifically, CIO duties should include:

- Translating strategic and user criteria into information network requirements.
- Setting technical standards so that providers know what is expected, commercial technology can be readily exploited, and information can be integrated.
- Ensuring criteria and standards are met in network designs and investment plans.
- Developing a multi-year network integration budget.
- Approving all network designs and investments.
- Refereeing competition and settling disputes.

To fulfill these responsibilities, the CIO must be a senior executive, reporting to the Secretary, able both to influence and to represent national defense strategy and resource priorities. The DOD CIO should be to information what the DOD comptroller is to money—both resources being vital to every aspect of national defense. At the same time, for the CIO to be an omniscient and omnipotent IT tsar would impose centralized organizational command over phenomena that we know flourish best when determined by user need, technological creativity, and economic forces.

Because DOD cannot function as a true market, the next best solution, as already noted, is to arrange business processes so that the allocation of resources and the development of solutions is determined by the demands of users. Service-managed network acquisition is not likely to satisfy operational needs that are inherently joint. For joint C4, it is only logical to treat the COCOMs as customers and the services as providers internal to DOD. Yet, the COCOMs, being regional and preoccupied with current activities, have neither global nor long-term perspectives, both of which are essential in setting and meeting

information requirements. There needs to be a global command charged with expressing the requirements of integrated information to support joint operations. This is consistent with the mandate of the Joint Forces Command (JFCOM), the top priority of which is, or should be, joint battle-management—C4. JFCOM should be the principal agent of the user community in investing in new information solutions while making service-based networks accessible.

Acting on behalf of the near- and long-term global needs of joint warfighters in the defense resource allocation process, JFCOM thus would identify the information capabilities required to fulfill the strategic criteria and user needs, as well as the resources needed to acquire these capabilities. This joint C4 requirement would compete for funding with other investment requirements (weapons, etc.) in the competitive arena of DOD budget preparation. In addition to giving the joint users a way to influence the network market, this would permit rational choice among alternative network investments to support operations. JFCOM could then invest directly in development and procurement of information solutions for key joint missions, e.g., strike, expeditionary assault, close air support, counter-insurgency operations, and counter-terrorist operations. Or it could call upon one or another service to meet the requirement, especially where the forces involved in the mission would be mainly from that service.

Such an approach raises questions about the existing legal mandate of the services (under Federal Title X) to equip the nation's military forces. However, given the centrality of joint C4 to force transformation and to network-centric concepts of operation, there is a strong case to be made for a special approach, not unlike the way that nuclear power and strategic weapons were managed early in the Cold War or the way Special Operations Command (SOCOM) forces are managed now.

However it is pursued, the goal of information integration for joint operations is more likely to be accomplished if first string IT networking firms are drawn into meeting the challenge and into direct contact with military users. While such firms may sell ordinary commercial products and services to DOD, they have been largely absent from the development of military network solutions. Yet, they have invaluable IT breadth, depth, and commercial experience. They also conduct advanced network-related R&D, fed by commercial revenues and global competition, on a scale vastly greater than what DOD can spend on the same possibilities. Both their market experience and their R&D are highly relevant to the problem of providing user-responsive information solutions. After all, information network firms, not defense systems contractors, propel this technology; enabling user accessibility and collaboration is their core business.

However, unless the DOD information network market is simpatico with the business model of the information network companies, it cannot compete with commercial lines of business within these firms for financial and human resources. Some long-established IT firms left the defense systems business; and the young lions of the Internet never entered it. This industry is geared to and dependent on a fast-paced dynamic market, not the sluggish and inflexible one of defense systems. But this is a cloud with a silver lining—by shortening the time and simplifying the process between identifying requirements and

delivering solutions, DOD can attract more of the IT industry into defense. That is exactly what defense needs to expand our forces capacities for information access and collaboration.

Thus, there are two powerful reasons for a reformed acquisition process, at least on the critical problem of creating joint user-responsive networking. A special C4 acquisition process—at least for joint C4 solutions—would give economic power and influence over solutions to network users while also eliminating disincentives to commercial network-solution providers. Of course, the goal should be to attract as many information network companies as possible, not just a dominant provider.

Traditional defense systems integrators could still play a useful role in understanding and translating operational needs while drawing on the networking skills and solutions of information technology firms. But they need not and should not be DOD's IT gatekeepers, which their privileged position as the only "qualified" prime contractors—so-called "lead systems integrators"—currently permits. Just as retail, financial services, and other sectors acquire solutions directly from the IT industry, DOD cannot afford to be insulated from the larger world of IT by a layer of specialized defense firms.

We wrote earlier of the economic shift that has occurred in the larger IT world over the past twenty years, favoring users over vendors, open over closed architectures, and networks over hierarchies. Acquisition reform targeted at giving joint users economic power and attracting network-solution firms to the defense market could produce a comparable wave and advance national security in the process. In addition to opening up external competition, internal competition should be fostered, up to a point. The structure of the external market for defense systems—several vendors competing for the business of a single customer (DOD)—could be replicated *within* DOD. More than one service could compete for the business of more unified and powerful joint customers. For example, both the Army and the Air Force could advance information solutions to the problem of tactical air-ground collaboration. This reinforces the argument for having JFCOM represent the near- and long-term needs of the entire warfighting community. The services, as well as defense and IT firms, would have strong incentives to gain joint acceptance of their C4 solutions. At the same time, internal competition for acceptance by the joint user community cannot go unsettled. As in any market, choices must be made, to the winners must go the spoils, and losers must be denied further funding.

Standards for network connectivity would be no less important under such conditions than they are now. Standards can emerge in several ways: (a) imposed by some authority; (b) established de facto by a dominant provider; and (c) a reflection of the demands of the user community.[19] The first way is inadequate; the second is to be avoided. Therefore, one of the most important functions of the CIO is to derive standards based on user demands—another reason for a strong link between the DOD CIO and the joint commands. Once determined, standards for military networks should not have to be

[19] Martin Libicki, *Standards: The Rough Road to the Common Byte*, (Washington, DC: National Defense University Press, May 1995.)

enforced. After all, failure to comply with standards in the commercial world is bad business, not criminal.

Standards serve as protocols whereby network solutions can respond to joint-user needs for information and collaboration across separate systems. Users will have no interest in networks that do not meet standards because they cannot help those users satisfy their criteria. It should not take long before providers realize that failure to meet standards will leave users dissatisfied and require either new networks or making existing systems accessible. Finally, standards should be tight where tightness is needed and not where looseness is desirable. As important as standards are for network connectivity protocols, they should not constrain solutions in which user creativity and diversity is important.

Knowing and Meeting User Demand

The centrality of user demands and the importance of being able to ascertain them are, by now, obvious. Users' needs for data and collaboration reflect the changing nature of operations, most which will be characterized in the future by:[20]

- Fast tempo.
- Depth of formations due to dispersion of forces and the distance between stand-off range and close-in fight.
- Non-linear and non-contiguous operations and forces.
- Irrelevance of inter-service seams in facing many challenges and opportunities.
- The requirement for time-urgent targeting.
- Simultaneous and parallel planning.
- Learning in action and adaptive decision-making.
- Letting humans focus on art-of-war decisions instead of managing information.
- Synergy between commander's intent and self-synchronization.

In DOD, users' network needs can be conveyed in four ways:

- combatant and other joint commands can specify them;
- separate services can glean them from forces serving under joint commands;
- the new DOD joint-force-planning process can derive them analytically and technically from the required capabilities for key joint missions;
- they can be inserted into the existing acquisition process whenever C4 investments are under consideration.

None of these can substitute for the kind of direct, continuous, two-way communication with users that providers need and that IT companies with extensive experience in commercial networking have come to expect. Moreover, the users themselves will not be patient with slow and filtered communication of their needs. Already, there is considerable anecdotal evidence that users are bypassing the established process and

[20] Description benefited from a brief by Bob Dees, Director of Defense Strategies for Microsoft Corporation. Brief entitled "Transformation & Interoperability through Integrated Innovation" (Microsoft).

going directly to the IT market—or simply to the Internet, despite its lack of security—or are jury-rigging their own solutions in order to satisfy access and collaboration needs.

This cry for help from what has been called the "under-privileged user" represents strong unmet need, with real military consequences. It means that network accessibility and related management shortcomings have already begun to exact a price in operational performance—a price that will only get steeper. Established regulated-bureaucratic processes to identify, fund, and meet requirements take too long and put too much distance between users and solution providers. This problem has long plagued users of weapons and platforms, and it is far worse when it comes to networks, given the rate of change of both technology and operational need.

Who, exactly, are the joint users? As noted, they are soldiers, sailors, airmen and marines. Apart from COCOMs and subordinate joint task force commands, they have neither structure nor voice.[21] The problem of finding the voice of the joint user is aggravated by the immaturity of joint-operational structures. The "component commanders" under the joint task force commander are essentially land, air, and maritime force commanders, trying their level best to improve jointness, but still wedded (if not welded) to their services. For instance, the maritime component combatant commander is likely to look to the U.S. Navy to furnish a battle-management network. While the component commanders are unlikely to be consistently good conveyors of joint warfighting needs, perhaps the insistence that those needs be expressed will transform the component commanders into genuine joint ones.

Whatever the process for specifying user needs, the concept of *smart-pull* should be paramount in the design and use of joint C4 solutions and the enhancement of existing networks.[22] From joint force commander to junior officer to non-commissioned officer, warfighters facing a specific task or threat should know best what information they need. While they should, in principle, have access to all information available via the network, they should neither be deluged with largely unhelpful information nor spoon-fed whatever information some headquarters staff decides they need, after having assessed and refined it. The network's information sources, many of whom are themselves users, should post information—raw as well as refined—and smart users should pull whatever they may find helpful. Intelligence providers and staffs may not feel that warfighters are smart enough to seek and use unprocessed information. The experience of the Internet suggests that those doubts are unfair.

As we shall see, the effective expression of needs of users for information, via smart-pull, can clarify the demand for IT solutions. Like all network users who are given the opportunity, warfighters will mold and mobilize information to fit recurring operating circumstances and needs. The truest expression of how best to furnish responsive

[21] Special Operations Forces are the exception.
[22] David Alberts and Richard Hayes, *Power to the Edge: Command… Control… in the Information Age,* CCRP Publications, June 2003. Available online at http://www.dodccrp.org/publications/pdf/Alberts_Power.pdf

information is to observe and listen to those who pull and shape it for their purposes. It has long been understood in the IT industry that the most effective R&D is that which is tuned to the frequency of the user. As responsive solutions are made available, they will in turn provide a way to transmit needs so that they can become more responsive still.

In DOD, there are "business" users in addition to warfighting users. The defense establishment could not function, and warfighters could not fight wars, were it not for effective personnel management, accounting and finance, installations, acquisition, logistics, and planning-programming-budgeting information systems. Because they were designed for specific functions, these networks cannot communicate with each other any better than combat networks can. Solving the defense business-network problem should be linked to solving the warfighting problem. The boundary between warfighting and DOD business is important and must be permeable. Poor access can be crippling. It is reported that the integration of reserve troops into stabilization operations in Iraq has been retarded by the poor responsiveness of pay and personnel data systems. While perhaps less urgent, these business systems should be drawn toward accessibility and collaboration by the same strategy that is aimed at improving responsiveness to and access of the warfighter. The users may differ, but the problem is basically the same.

Whether on the operational side or the business side, the real purpose is not to make military information networks interoperable but to make people interoperable and better informed. What matters is whether warfighters can instantly pull whatever information they need and collaborate readily with whichever other warfighters they choose.[23] In some cases, network-to-network interoperability may be feasible, economical, and necessary. In others, solutions may provide access to and communication with sundry networks that were not meant to be and do not have to be interoperable with one another. As we shall describe later, a unit in need of information should be able to pull it through a "directory" (or other search medium) that has access to various systems. For example, the air warfighter could learn about threats, munitions, targets, weather, available forces, and related air operations without regard for the interoperability of the systems that hold this information or for the information seams between tactical, operational, and strategic levels. This could make the existing base of information networks responsive and yield a continued return on the investment in them.

Feeling pressure from their warfighters, each of the several U.S. military services is already working on such an approach. But can we count on them to extend their solutions from service to joint? Returning to our simple air-operations example, the air warfighter *also* needs to know how ground forces want to make use of strike assets to take out critical targets and provide close support and how air strikes fit with missile and gun-ship operations. If joint warfighters cannot access data and communicate unhindered across service lines, information and instructions will have to travel up and down the line to and

[23] Increasingly, it will be systems, not actual people that pull information. For example, unmanned combat aerial vehicles (UCAVs) may call for off-board information that enables them to track and strike a target. Therefore, it might be said, strictly speaking, that warfighters—be they human or robotic—must be able to get whatever information they need and collaborate with whomever they must.

from the joint force commander—a reliance on hierarchy that loses the opportunity afforded by networking and misses the true virtue of jointness.

Because they hold component commands within joint forces, the services have a responsibility to provide cross-service communication and collaboration. However, it is safe to predict that they will do this by trying to open *their* service's network to others. At best, such an approach will solve the basic problem slowly, inefficiently, and inelegantly. Moreover, it leaves providers in control: like Ma Bell, the separate services define the need and decide how and how much to invest in meeting it. As noted, the priority a service places on joint C4 is unlikely to be as high as the priority it places on weapons platforms or as high as the priority the joint combatant commands place on joint C4.

At the end of the day, efforts to create information integration are all about operational outcomes. It is clear from Afghanistan and Iraq that joint operations—surveillance, clandestine entry, forced entry, strike, maneuver, and so on—can have decisive advantages. For instance, special operations forces can complement airborne surveillance to improve the effectiveness of air and missile strikes, which can create an opportunity to seize a sizeable land lodgment, which in turn can permit expanded joint maneuver operations, with close air support. In such operations, the contributions from and collaboration among various forces would be determined not by an inflexible prior plan but by adapting to unfolding conditions.

This is only possible with deployable, integrated, decentralized, and re-configurable joint C4. And that is only possible with networks that support such C4 qualities and that give units throughout the joint force unrestricted information access and collaborative opportunities—thus, information integration. To get to such a state, the combatant commands, galvanized and represented by JFCOM, need to lead an effort that starts with the information requirements of joint operations. That way, the needs of the warfighter, whatever the service insignia he or she wears, can be viewed through the lens of integrated operations and "rolled up" through a joint process of defining network-user needs and investing to meet them.

The question is whether the model generally outlined above would in fact produce such conditions of information integration. Would the alignment of investment resources and decision authority, and the scope for competition, including IT firms, be such that the capability to meet those requirements would see the light of day? Would solutions that fail to satisfy user-need criteria be disqualified? Would standards become welcome technical guidance rather than unevenly imposed rules? The final chapter of this volume will return to these questions after having reviewed current conditions within DOD and the rise of user-responsive technology.

II. Current DOD Network Development

Background

DOD ventured into information networks in the early 1980's and has been striving to enhance their utility ever since. Network evolution naturally followed separate service and agency funding channels, connecting users within hierarchical organizations: headquarters staffs, field units, agencies et al. The push to network across services gained momentum in the mid-1990s, inspired in part by lessons on joint operations from the first war with Iraq. Successive DOD strategic documents have called for better joint interoperability and full network integration across all forces, culminating in the goal of network-centricity as a fundamental feature of future concepts of operations.

While a secure and private Internet-like web is the goal, DOD is a long way from that ideal in all but a few specialized applications and organizations. Most actual data exchange—in Iraq, Afghanistan and elsewhere—remains hierarchical, push-broadcasted, and deliberately user-limited. Investment in modern computing and telecommunications systems alone will not create the desired transformation. That requires the build-out of a far more capable global backbone (now underway, as described below); unrestrained sharing among commands, services and units; and integrated information solutions, wherein every authorized user can access directly and instantly any information or other user on the network.

DOD's business processes and organizational culture have not evolved quickly enough to take full advantage of the current blossoming of user-responsive information integration. Service-centered biases and bureaucratic habits remain and reinforce one another as obstacles to collaborative investments in joint networking capabilities. At the same time, parochialism is not limited to the separate armed services. DOD's civilian staff, various agencies, and combatant commands all seek to protect and advance their own priorities.

Even by IT market standards, the scope of the defense network integration enterprise is huge. DOD data systems are comprised of approximately 3.5 million computers running thousands of applications over some 10,000 Local Area Networks (LANs) on 1,500 bases in 65 countries worldwide, connected by 120,000 telecom circuits supporting 35 major network systems over three router-based architectures transmitting unclassified, secret and top secret level information. And that is just the fixed-site profile. The most technologically challenging networks are those of deployed sea, air, land, Special Operation Forces (SOF) and space forces performing missions while in motion around the world, and their supporting intelligence networks.

Part of the problem is success. Since the dawn of the networking age (around the end of the Cold War), the U.S. military has achieved an impressive run of decisive military victories. In each experience—from the Gulf War to Bosnia and Kosovo to Afghanistan to Iraq—the advantages of enhanced awareness and collaboration have been more evident than the last. Just as information networking has not kept pace with the advance of technology, it has not kept pace with joint operational experience. Stories from recent

operations tell of tactical and operational communications cobbled together with existing assets and commercial wares purchased on the spot or express-mailed from retail stores back home. Even the commanders in the battle for Fallujah tell of relying mainly on cell phones and email (often unencrypted) as their primary means of communicating.

DOD divides its networking enterprise into three mission areas: business, operational and intelligence. Intelligence networks are not wholly managed by DOD but shared with other intelligence agencies. This chapter concentrates on DOD's operational networks, and to a lesser extent business networks. It describes how far DOD has gotten and how it is proceeding in its network-integration enterprise. It also identifies obstacles to progress.

Where DOD is Today

DOD directives over the past several years offer one way to measure DOD's efforts at managing and implementing network integrations to advance joint net-centric operations. A growing stream of official guidance establishes authority, direction, and method. It also indicates that DOD top-level management is trying to align its bureaucratic apparatus in support of the drive for joint networked operations.

Key points of reference for a strategy of joint networked operations are DOD's *National Defense Strategy* and the Chairman's *Joint Vision 2020*. These have been reinforced in recent years by other DOD policy documents, notably, the 2003 *Transformation Planning Guidance* (TPG). Below the conceptual level are a host of implementing policies, including *Interoperability and Supportability of National Security Systems and IT Systems* (2000)[24]; the *Joint Technical Architecture* (JTA); the *Joint Battle Management Command and Control* (JBMC2) Roadmap; and the *DOD Architecture Framework* in 2004. These and other references are essential for understanding DOD's commitment to, investment in, and method of pursuing network integration. These various writs have counterparts among DOD components, particularly the military services. Important as it is, this array of documentation reveals the bureaucratic complexity of the undertaking—at least the way DOD is going about it.

Federal government directives and legislation beyond DOD are also relevant. These show that Congress and the Executive Branch at large acknowledge the arrival of the information age in government and accept that the public sector no less than the private sector must update its practices accordingly. Their mandates require that DOD's goal of network integration must be department-wide and not confined to its military operational function. The main aim of these directives is to ensure that the government acquires and uses IT properly, which is quite different than transforming the way government functions in order to perform better by exploiting this technology.

In this vein, a key principle in adopting IT to government operations and managing IT costs is to define a clear link between IT investment and results, i.e., the return on investment for the taxpayer. (Ironically, the government is more self-conscious about getting a "good deal" in IT, when in fact it has benefited much less than the economy

[24] Chairman of the Joint Chiefs of Staff Instruction, CJCSI 6212.01B.

from the declining costs and growing productivity of this technology.) The key legislation and executive regulations are the *Clinger-Cohen Act* and *Federal Information Technology* (1996);[25] *Management of Federal Information Resources*[26] and the *Information Assurance Initiative* (2000); and the *E-Government Act* (2002). DOD appears to be in compliance with these laws and regulations, including early establishment of a DOD CIO reporting directly to the Secretary of Defense. Generally speaking, DOD compliance with government regulations regarding IT has little to do with harnessing it to improve military-operational performance.

In contrast to the commercial IT world, where the information revolution is as undocumented as it is unregulated, the directives and guidelines DOD has promulgated to bring about network integration are process-focused rather than results-focused. Many steps aim to ensure systems are non-duplicative, necessary and justified, best available solutions, and consistent with other initiatives. While these may all be appropriate strictures when making huge public investments, they add complexity, oversight, reporting, review, and compliance requirements. In short, DOD has applied its traditional processes, as well as government regulation, to networking. The commercial world has changed to realize the promise of IT; DOD has expected IT to conform to its world—a futile expectation.

DOD's approach may be bureaucratic, but its networking vision is bold: "an agile, robust, interoperable and collaborative DOD, where warfighters, business and intelligence users share knowledge on a secure, dependable and global network that enables excellent decision-making, effective operations and net-centric transformation."[27] This "global network" is to be a single, seamless interconnecting backbone of technologies over which many defined and self-defining collaborative networks will conduct DOD's business, some narrowly functional (e.g., nuclear propulsion engineering in the Navy), some service-specific (e.g., the Army's LandForceNet), and some broadly joint (e.g., CENTCOM's C2 network). In theory, any user can access all available information in real time, albeit depending on position and need.

Although some cross-boundary information communities exist, most networks still parallel existing organizational structure, be they service-, command- or agency-specific. Most information is not posted on networks until after it has been processed. Moreover, the standard practice remains to disseminate data only to selected pre-authorized users, as opposed to posting it for any interested user. Access to databases and networks is normally restricted, based on need-to-know as determined by the custodian of the information, not the user. A higher priority has been placed on the integrity and control of networks than on access and peer-to-peer use. If networks are to be accessed at all by an outside user, the outside user has to have host approval, effectively joining the network as

[25] Executive Order 13011 "Federal Information Technology," July 16, 1996.
[26] OMB Circular No. A-130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.
[27] Statements of Linton Wells II, Acting Assistant Secretary of Defense for Networks and Information Integration and DOD Chief Information Officer, before the House Armed Services Committee (Terrorism, Unconventional Threats, and Capabilities Subcommittee) 14 October 2004.

an internal user—a slow process at best. This is the norm, and change for the sake of joint integration will be impeded by security concerns.

Meanwhile, service elements collaborate selectively but increasingly in joint operations, and are hedging toward a need for full information integration. For example, Marine and Army forces accessed each other's UAVs and operated under the same command in Iraq. For the most part, however, service units and warfighters still operate mainly within their own domains at the tactical and operational levels of war. For bomber crews to take their targets directly from soldiers on the ground is still the exception, not the rule. And except for doctrinal close air support procedures, few units beyond Special Operations Forces routinely require joint information access and collaboration at the tactical level.

However, as the demand for integration grows, DOD's stock of existing, non-standard information systems presents a formidable challenge. Because mass replacement is too costly and impractical, DOD has opted for a graduated strategy, grouping existing systems under four categories to manage the transition to network integration: (1) starve existing systems that cannot economically be network-enabled (enforce aggressive migration); (2) enable existing systems that can be economically integrated; (3) sustain systems that conform with network standards; and (4) leverage DOD market strength to acquire open commercial-off-the-shelf (COTS) solutions—i.e., DOD users speaking to vendors with one voice to eliminate proprietary systems.

Building the Network

After no growth in investment in C4 in the 1990s, there has been significant growth since then. Major efforts to build global military network infrastructure are in train. Whether this will continue apace is uncertain. There is every indication that federal budget constraints will force tighter spending across DOD, including funds for network investments. Congress is likely to re-visit the issue of return on investment: tying cost to increased output. As noted earlier, this is harder to determine and show for C4 than it is for weapons and platforms, so there is a danger that C4 will be under-resourced relative to need and in favor of more visible (and politically attractive) combat systems.

In any case, DOD's network managers and providers will have to prioritize their plans for systems acquisition and deployment. Two tenets will, or in our view should, dominate the choices. First, the incorporation of proper, network-standard IT in important future systems (e.g., the Joint Strike Fighter) should not be sacrificed, which would create information disconnects for major capabilities down the road. Second, priority acquisition of network infrastructure should go forward with minimal delay. In addition, tactical-level joint systems, such as Blue Force Tracking, are so highly prized in the field that cuts or delays are unlikely. In short, even in a more austere funding climate, investments that further information and operational integration can be sustained.

What follows is a brief description of major capabilities and programs that bear on network robustness, reach and integration, starting with the GIG. Assembled and coordinated by the Defense Information Systems Agency (DISA), the GIG is "the

globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel." The GIG includes DOD-owned as well as leased communications, computing systems and services, software, data, network services. Within the GIG, each of the armed services furnishes its own applications, services, and operating networks—like specialized shops within a common factory.

The GIG supports DOD, the intelligence community, and other parts of the national security establishment in peace and war. It provides capabilities to operate locally, regionally, worldwide, in space, with non-DOD users, and with non-US forces and networks. The GIG operates over three IP-based router-defined networks for unclassified, secret and top secret data. Security is provided by separation from the global Internet. GIG networks are maintained by DISA and operated by the Joint Task Force for Global Net Operations (JTF-GNO) under the joint Strategic Command (STRATCOM). In order to ensure tight linkage between maintaining and operating the GIG, the Director of DISA is dual-hatted as the Commander, JTF-GNO, and the two organizations are co-located.

Extending the GIG to all users is DOD's networking highest priority. Five key initiatives comprise that effort:

Global Information Grid—Bandwidth Expansion (GIG-BE)
GIG-BE is the terrestrial component of the GIG. Developed and maintained by DISA, GIG-BE consists of 92 sites worldwide and is operated by JTF-GNO. Six sites achieved initial operational capability in September 2004. The remaining sites became operational in September 2005. GIG-BE supports all COCOMs and intelligence users, and also is linked to DOD business operations and data repositories supporting warfighters and other users.

Transformational Satellite Communications (TSAT)
TSAT is the future space-based portion of the GIG, counterpart of the terrestrial GIG-BE system. TSAT is essential to extension of high data-rate and advanced communications to mobile and tactical users. It will employ laser technologies to bring very high bandwidth up and down links to GIG users via optical IP-based communications. It should be operational in 2007.

Joint Tactical Radio System (JTRS)
JTRS is a multi-service program that will bring IP-based data and voice communications to mobile users. The JTRS revolutionary software-programmable architecture will allow users to operate almost anywhere along the frequency spectrum. This is principally an operational-tactical-level data exchange system that can be rapidly reprogrammed to facilitate units being redeployed from one joint operations area to another. Fielding has been long-delayed since the system was approved in 1996 and remains uncertain. The first operational units are to be deployed in 2008—at least a dozen long years from inception.

Net-Centric Enterprise Services (NCES)
NCES is a DISA-run system intended to facilitate access to a common operational information and network collaboration by providing a host of mission-critical information to all users anywhere, anytime. NCES is the cluster of services that will transition DOD from its current platform-centric IT system to a network-centric system; from a time consuming and limited access "push" information system of Task-Process-Exploit-Disseminate (TPED) to a real time, "pull" information system of Task-Post-Process-Use (TPPU). Because information will reside on the network and be universally available, it will only be handled once. The nine core NCES services are: information storage; information discovery; instant messaging; user collaboration; information assurance and security; enterprise services management; applications; user mediation; and user assistance. NCES will be run roughly analogous to a typical network system administrator-and-help services concept. NCES is early in its development; however some core services will be fielded along with GIG-BE rollout at the end of 2005. Afterward, the system will go through a series of upgrades in quality and availability of services as new technologies and operational experience yield better ways to collaborate.

Information Assurance (GIG-IA)
Information assurance is critical to gaining user confidence in a secure, dependable and accurate GIG. GIG-IA is especially critical to DOD IT networks, both in terms of their reliability and security from attack. The Security Management Architecture encompasses all traditional security services and a related Security Management Infrastructure. Requirements for GIG-IA were validated in late 2004 and the proposed GIG-IA infrastructure is under review.

Taken together, these investments will go far toward putting in place the infrastructure for information integration in support of operating forces. Just as land- and space-based augmentation of the GIG will extend band-width to users, NCES will help users exploit the infrastructure. These programs are necessary, but they are not sufficient. Whether, how and when warfighters are really afforded access to whatever data they need when they need it, and are able to collaborate spontaneously with any units that need or can provide support, depend on DOD's organizational ability to harness the power of user-responsive methods and technologies that are sweeping across the world at large. DOD's non-market business processes may not obstruct investment in underlying infrastructure. However, unleashing the capacity of this infrastructure for the benefit of warfighters in joint operations will be a greater challenge for DOD, requiring unprecedented organizational flexibility and alignment of economic power with user demand.

Network Integration Governance and Management at DOD

Two principal staffs drive network integration for DOD. The primary DOD manager is the Assistant Secretary of Defense for Networks and Information Integration (ASD for NII) who is dual-hatted as the DOD CIO—a direct subordinate of the Secretary of Defense as required under the Clinger-Cohen Act. The CIO sets standards, tracks interoperability and oversees compliance with joint architectures intended to achieve

network integration. Supporting the CIO is DISA, which is the agency responsible for developing and managing DOD's worldwide backbone network infrastructure.[28]

The primary agent for determining the joint requirements of the combatant commands and getting them into the acquisition system is the Joint Staff Director for Command, Control, Communications and Computers (JS J-6), who is also designated as the joint community's CIO. The J-6 represents the COCOMs in the JCIDS and in the JROC (Joint Requirements Oversight Committee) on matters of C4, including networks.

JFCOM is responsible for joint-force integration, including network integration among the military services and in the interagency and multinational arenas. In this capacity, JFCOM consolidates and harmonizes network requirements of the combatant commands and works with the J6 to ensure, through JCIDS, that service investments in network systems include interoperability criteria as part of any approved system design.

What JFCOM is to planning joint-operational network capabilities, STRATCOM is to operating them. STRATCOM has been assigned responsibility for Information Operations and Global C4ISR, including responsibility to operate and defend the GIG. JTF-GNO is a component command of STRATCOM, uniquely provided by a defense agency (DISA) rather than a military department. STRATCOM is both a war-fighting command and a supporting command to the regional COCOMs in terms of providing GIG support for their networking requirements. Along with JFCOM, STRATCOM sits on the DOD CIO Executive Board.

The military services are responsible for equipping their forces, including equipping them to be jointly capable. That means investing in systems that meet standard connectivity protocols promulgated by the CIO for all U.S. military forces to be able to operate in a joint environment. There are substantial costs to meeting these technical interoperability requirements, which the services must trade off against other priorities as they allocate money. While the services give every outward indication of commitment to achieving network integration as soon as possible, timelines are not hard and fast, and funding is a major factor in determining progress.

The services are focused on fielding their respective portions of the GIG, relying on network "boundary interfaces" to reach across the joint backbone to other service users. Fortunately, many service units operate under only one COCOM. Problems are more acute when a major operation, like Operation Iraqi Freedom, calls for unfamiliar units to work for a COCOM. A service's forces can be in compliance yet disconnected at the same time because technical standards include different options for every connectivity medium. Practically speaking, the Office of the Secretary of Defense (OSD) cannot remove older options or deny new technologies precipitously. It takes time, money and emphasis to effect change. If a service believes its priorities lie elsewhere, connectivity upgrades may be deferred and integration might suffer when units are deployed.

[28] DISA is responsible for network infrastructure only up to gateways in the various regions or theaters and only up to bases not on them. Thus, DISA's current responsibilities do not extend all the way to the tactical or end user.

The COCOMs are the users of operational networks in the field. The needs of the COCOMs reach the requirements process through various filters. JFCOM determines requirements through joint experimentation. Joint requirements can also be forwarded through COCOM component commands to their parent service. The J-6 can also identify joint requirements. COCOMs are provided the opportunity to review before approval any JROC decision or J-6 interoperability certification. Most COCOM communication and information networks are traditional hierarchical systems tethered to fixed locations, relay sites or satellites. These are managed and controlled by the COCOM J-6s.

Network integration, like other high-priority and high-visibility investments, attracts many influential external actors. Congress is keenly interested in networks that bring greater joint-operational capabilities. However, Congress is also sensitive to the high cost of IT systems in DOD (and across the government)—in contrast to rapidly dropping IT costs in commercial sectors—as evident by legislation that seeks to ensure sufficient return on investments in all areas of government IT.

Other external actors include the full array of defense systems contractors, some IT software and hardware firms, the policy-analysis community, and international bodies. In NATO, analogous integration architectures and standards have been defined, are the subjects of considerable investment, and must be standardized with at least the main U.S. networks technologies. A new factor, not yet defined, is the emergent cluster of interagency and intergovernmental departments that need to network with DOD at all operational levels for homeland security (e.g., DHS) and overseas stability and reconstruction (S&R) operations (e.g., State, USAID). This last group of actors has a whole different set of network protocols, often unencrypted, commercial, cellular, satellite and Internet-based. Nonetheless, the J-6 is responsible for identifying and determining the interoperability requirements of interagency networks of interest to DOD users.

Standards

Adherence to connectivity standards is essential for systems interoperability, which has been necessary for information integration. The CIO is responsible for the negotiation and promulgation of standards. In determining standards, the CIO works via committees that include the services, COCOMs, J6, JFCOM, DISA, and the DOD acquisition community. The principal committee is the DOD CIO Executive Board (CIOEB), on which JFCOM, STRATCOM and J-6 are the members most involved in speaking for the COCOM user community. DISA is the DOD executive agent for information technology standards; for that function, it has a Center for Standards, which works with the CIO, Joint Staff (J-6), and the armed services.

The JTA was conceived in the early 1990s and first issued in 1996. The 6th version was published in late 2003. The JTA sets and disseminates profiles for IT standards intended to achieve interoperability as new technologies become available for DOD use. There is a conscious effort to incorporate technological advances, and DOD subscribes to the principle of maximum use of commercial systems that include these advances. However,

the pace of new technologies and the slow DOD bureaucratic process of standards negotiation are often out of sync. The standards process is tedious and the JTA has become a ponderous tome. Even as accommodation of new and useful commercial IT offerings generates new standards for systems to adhere to, DOD finds it much harder to eliminate old standards because many legacy systems remain in use throughout the forces. The need for streamlining the standards process is generally acknowledged. Adding new protocols without shedding old ones increases the compliance burden of both legacy and new systems. This widening gap has increased emphasis on standardizing data (by means of metadata or tagging) to flow among dissimilar technical systems, rather than attempting to make so many technical systems themselves compatible.

The interoperability problem can be exacerbated by the phenomenon of churn—investing in new systems mainly because they are the latest commercially available, even if only marginally better than older systems. The practice of establishing "refresh cycles" for IT systems, based on pre-determined multi-year increments, is meant to allow better fiscal management and to reduce churn. If new standards are to be incorporated expeditiously, DOD may have to fence funds to select programs solely for standards conformance.

Tension is growing between users' demand for rapid fielding of useful information systems and the need for standards compliance. In Iraq, for example, the Army and Marines employed different Blue Force Tracking systems, one satellite-linked and other radio-based. They were not compatible. DOD is now engaged in merging these systems into a Joint Blue Force Situational Awareness system. But how did jointly incompatible systems get to the field in the first place with a standards oversight system in place? Either waivers were approved or the services invoked one of many so-called "rapid procurement" buys, and/or COCOMs by-passed the acquisition and standards-review system.

Acquiring Systems for Network Integration

Title 10 of the U.S. Code establishes an Under Secretary of Defense for Acquisition, Technology and Logistics (USD/AT&L), and DOD Directive 5000.1 identifies USD/AT&L as the civilian executive responsible for supervising all DOD acquisitions. The military departments have delegated responsibility for all acquisitions within their respective components to an assistant secretary, known as the component acquisition executive (CAE). Within this framework, most non-urgent network-related acquisitions are acquired by the service CAE's, by SOCOM, which has unique combatant command Title 10 acquisition authority, and by DISA, which has its own acquisition authority as a DOD agency. This is a methodical, unhurried process marked by public solicitation, competitive sourcing, appeals, full documentation and accounting, and auditing oversight.

All civilian and military agencies across DOD participate in the formal acquisition process, which generally follows a two-year cycle. Strategic assessments are made though the Joint Strategic Planning System (JSPS), and integrated capabilities are defined

and developed by the JCIDS. Paralleling the JSPS is the civilian-managed Planning, Programming, Budgeting and Execution (PPBE) process, overseen by the Deputy Secretary of Defense. Finally, the Defense Acquisition System (DAS), overseen by the Defense Acquisition Board (DAB), makes decisions to acquire any given system.

These processes are in theory sequential; however, they are interactive in practice, as a proposed capability works its way through the entire framework. Both IT network systems and other systems go through these processes the same way, with approval for advancement to the next step determined by governing bodies comprised of all relevant stakeholders. The primary governing councils are the JROC and the DAB. The CIO Executive Board and/or the Information Technology Acquisition Board (ITAB) govern network acquisitions. In the case of network systems, interoperability with other systems (e.g., those being acquired by the other services) is tracked throughout the entire process.

It is evident from the brief overview above that the acquisition process for IT and other capabilities is long, complex, and inflexible. A given network acquisition relating to joint C4 could involve multiple actors (CAE, COCOM, AT&L, JFCOM, CIO, STRATCOM, DISA, J-6) and multiple committees (DAB, JROC, CIOEB, ITAB) with overlapping memberships and jurisdictions. The requirement to coordinate with many actors makes network acquisitions if anything more complicated than other acquisitions—the opposite of what the user needs and the market offers. To some degree, this is part and parcel of making huge public investments that affect national security—they should be transparent, fair, and open to challenge. However, in view of the pace of IT markets and developments, there is a search for ways to speed network-related acquisitions and make them more like the nimble procurement seen in the private sector. (In reality, not all private sector acquisitions, particularly for large corporations, are storied examples of rapid and successful acquisition). A major frustration with the DOD system is that many rules have been put in place primarily to prevent abuse and provide for congressional oversight rather than to make wise and expeditious decisions. Once in place, it is very difficult to change rules due to inherent organizational inertia and even overt resistance, even if a rule no longer represents sound management practices.

Users are important but are not the driving pivotal voice in DOD's formal acquisition process. COCOMs do not sit on most councils where acquisition decisions are made, though they are spoken for by two joint advocates: J-6 and JFCOM. To date, J-6 has been the main representative for the COCOMs, except on the DOD CIO Executive Board where JFCOM and STRATCOM also participate. The COCOMs can also review and comment on any JROC decision or JFCOM joint-interoperability certification.

An interesting provision of DOD regulations and related legislation is a procedure called Other Transaction Authority (OTA). OTA was instituted in 1989 to simplify DOD contracting rules to allow smaller companies to face less complex compliance burdens with regard to accounting, competition and auditing. The practice soon became popular not just among small newcomers to DOD procurement but older more established vendors as well.

"Rapid Acquisition" is a catchall phrase referring to virtually any procurement method that short cuts the formal DOD process. There are several such schemes. The use of special operational funds, end-of-year funds, supplemental funds, experimental project funds, activation funds and commanders' initiative funds are some of the ways both COCOMs and services can quickly acquire limited quantities of a desired item.

Rapid acquisition practices are increasingly common. Estimates of how much such procurement occurs in network-related systems are as high as 30 percent. Industry representatives call on commanders or invite them to demonstrations of experimental technologies. Units readying for deployment discover their equipment is not compatible with that of the units with which they must interoperate—a particular problem seen as more and more reserve units go to Iraq, where they have never before had a command relationship or mission focus. In such cases, the COCOM often becomes the IT provider for a particular unit or operation, as hurried pre-deployment acquisitions are pushed through, often collaborating with the unit's parent service for funding.

Two drawbacks of rapid acquisitions have surfaced. First, such systems may solve immediate network requirements but they can lead to incompatibilities, especially if the force so equipped is redeployed to another theater where the acquired system is not in use. Second, technical and logistical support for non-standard systems may not be assured, especially after the mission is complete and the unit carries the new system home expecting to use standard supply channels.

The problems of rapid acquisition aside, there is an inherent tension between the speed with which the commercial IT sector produces new, more capable technology and the methodical DOD processes for spending public money. This friction can and should be alleviated, in particular for systems with immediate and obvious benefit to warfighters. Of course, big-ticket network systems will inevitably attract close scrutiny. At the same time, as already noted, large multi-year acquisition programs, with their inflexibility and management overhead, are not suitable for acquiring most information solutions.

DOD has recognized the need for rapid acquisition in the current wartime environment and created a cell dedicated to rapid acquisitions of all systems. The Joint Rapid Action Cell (JRAC) is co-chaired by directors from the DOD Comptroller and USD (AT&L) and reports directly to the Deputy Secretary of Defense. Any flag officer can certify a request in the field, which is validated by the Joint Staff. Requests are to be met within 120 days. JRAC was set up in late 2004 and is enjoying a high level of success in meeting its 120-day standard. However, the focus is primarily on urgent warfighting needs such as body armor or specialized ammunition—items already in the system but in short supply.

In one recent example of rapid network acquisition, the Army provided the Joint Network Node (JNN) system to its first modular force, the 3rd Infantry Division, redeploying to Iraq in late 2004. The entire process from design to fielding took under six months. JNN includes voice-over-IP and mobile Internet technology. It is presently being fielded to other divisions.

Thus, acquisition can be sped up by exception to the normal process. Rapid acquisition is designed mainly to hasten delivery of capabilities to deployed and deploying units. This is, of course, a very different rationale than providing for acquisition at a pace and in a way that can take advantage of the fast "turning" of IT and IT markets. The distinction between urgency and relevancy is important. Take the information suite of a new combat aircraft (e.g., F-22 or F-35). With much work yet to be done on the airframe, propulsion, and other sub-systems, there may be no rush in acquiring onboard IT to fit joint networks; so rapid acquisition is irrelevant. However, it is crucial that the aircraft is not locked into IT systems that cannot change continually as technology changes. What matters in such a case is not only the speed but also the flexibility and frequency with which an information system is acquired and updated.

In sum, it is not clear that a highly regulated and deliberate acquisition system can, even by providing short cuts and waivers, be reconciled with the rapidly changing demands and technological progress of the information world. The fact of exceptions indicates that the existing system is not conducive; yet exceptions alone will not cure the problem. Nor is it clear, though, that "de-control" and acceleration of IT acquisition can be squared with norms of public procurement. We will return to this conundrum in the final chapter.

Obstacles to Progress

1. Service Parochialism

DOD's programmatic system remains as it was before operational jointness became national strategy—legislatively established along service lines that create a by-product of service bias that can frustrate jointness. The programmatic system is also characterized by the uncertainty of funding throughout the entire life of any major investments. The inevitable unknowns about cost growth, required quantities, and production stretch-outs haunt program managers every step of the way. These realities trigger much of the fierce *en garde* posture service program managers and senior leaders assume in protecting existing programs and budgets. Blatant parochialism—the unabashed belief that any one service is genuinely more capable, worthy or important to national defense—has largely disappeared over the 19 years since Goldwater-Nichols. But it would be naive to think that no vestiges persist.

What remains is a subterranean seam of parochialism. This is the so-called "iron middle" of service staffs, both uniform and civilian, concentrated especially in the programmatic and budgetary arenas. Not unimportant to this is the reality that each service gets a finite portion of the defense procurement budget and must produce the maximum service-particular capabilities from those resources. Choices have to be made, and one rational choice for a service is not to favor expenditures when the requirement is for capabilities beyond the service itself (i.e., joint capabilities).

The services are not unique in bringing bias into their budgetary decision mix. For example, COCOMs have an understandable bias in favor of the immediate needs of the warfighter over investment in capabilities that anticipate possible future challenges. An important analytical question is whether the rapid speed of advancement of IT and of user

desires is compressing time to the point that future needs are well represented in immediate ones (or, alternatively, that it is next to impossible to look out beyond a few years). The experience of the Internet, especially in regard to search and user-reach capabilities, suggests that, to some extent, "the future is now." This phenomenon would reinforce the view that COCOM needs are a sound basis for development and acquisition, though COCOMs would still be susceptible to regional bias.

2. The Added Costs of Jointness

The high cost of any program is one of the most sensitive aspects for services concerned with funding scarcity. Once a program has won hard-fought approval, program managers focus understandably on reaching operational capability in the numbers of systems approved at the stated cost and on schedule. As cost overruns invariably occur in development and production, savings are sought by eliminating features. Jointness can increase cost or cause delays as technical approaches to connectivity protocols are developed and tested.

From a service perspective, if DOD or Congress mandates information integration, specific funding should be added to the program to enable it. Typically, added funds are not provided, and the increased per unit-cost means either fewer units or the sacrifice of other features. Until the recent emphasis on integration, there was little commitment to interoperability requirements, making the choice to eliminate those capabilities all too easy for service program managers.

3. Frequent Waivers from Agreed Standards

Service requests for waivers from JTA standards, as well as operational and systems standards, are frequent and usually approved. Most waivers are granted for rapid acquisition of non-standard COTS purchases intended for immediate fielding with deployed or deploying forces. The practice has become more or less pro forma in the expanding area of rapid acquisition. The longer-term effect, however, is to delay and increase the cost of achieving an integrated, supportable union of networks.

Perhaps the greatest impairment continues to be the large inventory of existing systems that are not jointly compatible simply because each service or agency developed its networks in isolation. As long as these old systems stay in the inventory, connectivity with them is a mandatory design feature of any new system. This, too, slows integration.

4. Cultural Resistance

Cultural obstacles run deep and are the hardest to overcome. The adage that "information is power" is universally accepted. However, DOD's determined shift to future network-centric operations and warfare (NCOW) involves more radical ideas. One piece of net-centric culture-shock is "*post-before-processing*." Traditionally, data is processed first—its utility determined and exploited—and then disseminated to others (usually pre-approved others). Streaming data to all interested users on a network surrenders a degree of control and the chance to present the information to others when and how one deems best. Unmanned sensors pose no problem in this regard, but human collectors will need to change the way they think: posting unit locations, personnel and equipment status,

situation reporting, even identifying enemy positions and capabilities cede some control over the immediate situation.

A related cross-cultural net-centric concept is *unrestrained information sharing*. Net-centricity requires information sharing based on "communities of interest," without regard to organizational boundaries. Without a universal willingness to share information, being connected will have diminished value. Today, information is shared only within a defined organizational stovepipe; users do not know much of what goes on beyond their parent organization. Cultivating informal contacts in other organizations is customary because it affords a broader picture and faster access to information.

A third net-centric principle that runs against the grain is manifest in NCES. That is, users must rely on enterprise services for all information. This is analogous to having no files on ones own hard drive; all information is on an office network server. The Only-Handle-Information-Once (OHIO) tenet means that there will not be multiple collections of the same information; once acquired, information will be maintained, updated and available for every user via NCES. Today, most individual users gather and maintain stand-alone databases to some degree. That injects duplication and errors, slowing collaboration and diluting the combat power of networking.

These are some of the more daunting cultural obstacles to information integration. Along with service bias, they could pose significant brakes on progress toward user-responsive information solutions and network-centric operational integration.

5. Policy and Process Problems

Each of the services still has a lot of work to do to harmonize its internal policies for joint operations in the area of joint networking. The simple yet dissimilar ways units or services accomplish tasks can become disabling when forces must share information in order to collaborate. A common attitude is: we have always done it this way and would have to go to considerable expense to change our entire system. Better to wait and see if you can make the other guy change his system.

Again, take the example of the Army and Marine Corps working together in Iraq. While UAV data apparently could be made available across service lines, unit-location data could not because one service had a policy that prohibited sharing that data with entities outside the unit itself and its chain of command. The result was that location data (Blue Force Tracking) was not available for policy reasons rather than a lack of compliance with standards. Similar procedural obstacles to sharing information can be discovered up and down and across the Department of Defense structure.

6. Network Access and Control

The ideal of "any user able to access all information on the network in real time" is at cross currents with traditional network control and the principle of "need to know." Typically, control resides with the highest headquarters on the network, which can decide who may enter. Owners of databases similarly screen those seeking access, though that problem can more readily be automated. Most authentication procedures are rigorous:

Are you who you say you are? What is your clearance level? Why do you need to know? Even within the Pentagon, one is not given access to selected networks and data merely because one has appropriate clearances and equivalent technology. The same is true throughout DOD and even within each service. A system administrator issues user name and password after access is approved. COCOMs adhere to similar formalities at the field and fleet operational level. A command wants to know who is on its networks.

There are sound reasons for established practices of network control. Moreover, the expansion of networks makes integrity both more difficult and more important, in that the probability of an enemy being in the user population increases as the user population increases. This dilemma will have to be addressed if DOD is to come into a union of networks whereby any user is able to access any useful information. As unit operational locations are automatically reported via Blue Force Tracking technologies, can any DOD-wide user access that data? Does a unit planning an operation have to be concerned that its plans and locations are known beyond who ought to know? What does this do to operational security?

DOD has yet to grapple philosophically with how to reconcile the vision of unobstructed access and collaboration with the deeply entrenched idea of controlled access. Presumably users would only seek information they need operationally. Would users at the unit's home station in the United States be tempted to access location data to learn if their comrades are in or out of harm's way? We know that today many users are family members of other users. Do we want any interested user to access the target information the night before a strike? The bomb damage assessment after a strike? Of course not. Will commanders willingly post before processing their unit's situation reports, maintenance status or readiness levels? Will they be concerned that their own superiors could get such information from other sources before they can present it with appropriate comment themselves?

NCES will populate the network with applications, provide assistance to users, instant messaging capabilities, system security and information search services, and offer collaboration tools. It is axiomatic that systems security means knowing when unauthorized actors attempt to enter the net. That means knowing who is an authorized user. In turn, that means an authorization regime of some kind that meets the needs of both information security and user responsiveness.

Concluding Observations about the Status Quo

DOD is making some progress toward its networking goals. Today, joint network operations are favored by the military's most senior leaders. Moreover, the next generation of leaders, being seasoned in places like the Balkans, Afghanistan and Iraq, is impatient to see a truly joint networked force materialize. Some key factors in nurturing a cultural shift toward broader sharing and collaboration and breaking down old paradigms have been the advent in joint education, a wealth of commercial best practices and, of course, the Internet's ubiquitous presence in everyday life. Today's military decision-

makers, whatever their level, demand to be connected continuously to whatever data systems and users they believe essential to their mission.

Across DOD, there is heavy investment in the infrastructure needed to enhance and integrate C4, with numerous commands, staffs, agencies and contractors committed to the goal. Growing effort to achieve some network integration is already in place, albeit mainly within the services and defense agencies. There is notably less progress across joint forces, particularly beneath the joint-task-force command level. But key joint networks are being developed and have already become the strategic and operational backbone for the war on terrorism.

Although the goal of integration is recognized and accepted, pockets within all services cling to higher priorities than joint integration when it comes to IT investments, not to mention other demands on resources. Such resistance should gradually die out as the forcing mechanism of connectivity drives operating commands and users to insist on joint information integration. The question for the remainder of this study is whether a gradual rise of user power can and must be accelerated by altering processes and governance.

All do not see the same extent and depth of network integration necessary for military operations. Some question whether the promises of net-centricity are exaggerated. Will universal access to information yield a common operational picture and self-synchronizing organizations, as claimed, or will different users interpret what they garner from the network in different ways? How will conflicting information be resolved? Will the right forces 'self-synchronize' depending on operational demands, or will differing camps coalesce around alternative operational solutions? How will peer-to-peer networks overlay traditional command and control?

Thus far, the pattern has been to use networks to enable existing organizational structures to access and distribute better information. That, of course, is well short of the revolutionary use and impact of the Internet and other solutions that are dominated by user needs for access and collaboration, as determined by users. In short, the hard part for DOD is yet to come.

Of all the problems associated with bringing DOD and the world of user-driven network technology into harmony, two contradictions stand out. The first is that the regular defense acquisition system, even with use of fast-track exceptions, cannot keep pace with either the generation of or the demand for the technology in the larger economy. The second is that expanded access and collaboration collides with both the ingrained habits of and good reasons for information security and network integrity. Just try to access another service's databases or enter a network (or even in your own service) that is beyond your hierarchical organization. We will come back to these challenges after looking at developments in the wider world.

III. User-Responsive Information Technology Development

Redefining Integration

As is clear by now, DOD, like much of corporate America, has long suffered with the difficulties of achieving seamless integration of disparate information systems. Issues and phrases such as stovepipes, requirements processes, boundary interfaces, and interoperability clutter conversations throughout the Department and the services, and make the life of the CIO unenviable. However, since the late 1990's, commercial information technology advances, along with some elegant thinking about approaches to information integration, call into question the validity of a number of precepts. System interoperability may be a dated concept. Structured requirements, voluminous documentation of software code, and extensive training are yielding to user-defined views and continuous redefinition of "The System."

The definition of a system integrator is also being recast. In many instances, like those cited below, information integration is now being achieved by small in-house teams in complex environments in a very short period. Existing systems were not asked to "talk" to one another; they were simply required to produce live feeds of data. Therein lies the opportunity for DOD to adjust its relationship with its major contractors, change the economics of information technology, and agilely adapt to new circumstances.

Information Integration - A Private Sector Case Study

The Washington Hospital Center (WHC), the flagship teaching hospital of MedStar Health, is the largest hospital in the Washington, D.C. area, and serves more than 250,000 patients each year.[29] The ability to access information quickly from a myriad number of sources, formats, types, locations, etc. is critical to patient care and to the efficient operation of the business aspects of the institution. However, it could take hours to retrieve a paper based patient record, lab results, and x-ray films. The electronic storage of these sorts if data is an obvious solution, but such systems bring with them the need to integrate disparate systems and provide an interface to users both intuitive and appropriate for the task.

In 1995, the WHC recruited Drs. Mark Smith and Craig Feied to attack the problem of information integration and availability for the Hospital's emergency room. "We identified 300 data islands within the medical center," says Dr. Feied. "Patient registration information was locked up in one system, while lab reports where in another, radiology readings from digital x-rays were in one format, CAT scans were in another, and electrocardiograms in another. The list goes on and on-300 different systems that couldn't talk to one another." The effect of this predicament on the daily lives of the medical staff, support and administration organizations and, most importantly, patients was far reaching. Revenue was lost through loss of patients records, wait times for

[29] There are several articles about the Washington Hospital Center's approach to information integration. Much of the information throughout this section was obtained from a Microsoft Case Study and which is available at: http://www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=14967

patients stretched into hours, which in turn lead to crowding and a perceived need for facility expansion.

In 1996, after thirteen months of development, the InSight system was launched. Using commercial systems such as the .Netdevelopment system, the WHC team created an object wrapper interface that collects a real time copy of each new data element, places an XML wrapper[30] around the data, parses it and stores it within a server. This is done for every system that produces data. There are several fundamental tenets of the design:

- Datum as simple as a temperature reading or as complex as digital x-rays or voice recordings are all treated as "data atoms."
- There is no presumption made about what data is important to know and what data is not important.
- The user defines the view of the data as they choose. There is no presumption on the part of the system as to what view is appropriate.
- The code is by design, undocumented. Given a strong adherence to object software principles, it has been found easier and quicker to rewrite a piece of code than try to decipher a previous developer's intent.
- The system is used with minimal training.

The operational metrics for InSight are telling:

- The data store, spread across a number of servers totals about 13 terabytes for a single hospital and is growing at a rate of about four terabytes per fully instrumental hospital.
- Patient information queries are responded to in about one-eighth of a second.
- Approximately 20 percent of the code is rewritten each year, allowing new functionality to emerge over time as the code base is constantly updated.
- Approximately one-third of the hardware is replaced each year.
- Significant attention is paid to security of information.
- Only two hours of downtime since the system was launched in December 1996.
- The system has been migrated to the entire MedStar chain and to approximately 50 unaffiliated hospitals.

This remarkable solution was architected, created and supported by Drs. Smith and Feied with only two or three support staff. It is maintained by a similarly small team. When a new data source is acquired, it is typically incorporated into the system within days. The introduction of the system into another hospital, typically takes a month or less.

The benefits of the system are profound:

- Patient care significantly improved and, with data easily accessible across patients and across hospitals, much deeper insight is gained into cause and effect.
- Revenue to the hospital significantly increased.
- Emergency room capacity throughout the system doubled without an increase in staff or facilities.

[30] XML: Extensible Mark-up Language standard

- Capability for bio-surveillance developed as data across hospitals is aggregated.

"Their system is a monumental achievement," says Jonathan Handler, MD, Director of Informatics and Assistant Professor at Northwestern University, Division of Emergency Medicine. "Nothing has ever been done like this before. It completely transforms the experience of treating patients and what you can do for patients. Medicine has never had a system like this, which collects every drop of clinical information and puts it into the hands of physicians, to help them make the right decisions—more quickly, and more efficiently."

"The old way was a nightmare for the cardiologists because they had to go to a special viewing place, and then they were looking at the images without the context of the other patient information," Dr. Feied says. "We wrote new code to import the data and store it as a BLOB (binary large object) in a SQL Server field. Within two weeks, we rolled out the new module. One click, and within an eighth of a second, you are watching the heart pumping."

At this point, it is worth contrasting the success at the WHC and more traditional IT projects.

- The team was small.
- The time was short.
- Documentation was ignored.[31].
- Software disposability was embraced. Rather than a cumbersome change control process, software was designed to be replaced as new opportunities to improve functionality.
- Similarly, the planned obsolescence of hardware has been found to be economical as prices continue to drop and functionality improves.

The role of the systems integrator, at least at the WHC, has been radically redefined.

The success achieved by the WHC team rests on four pillars:

- Solution conceived from the vantage point of the end user.
- A fundamental questioning of the tenets of traditional information design.
- The availability of modern software developments.
- An enlightened hospital leadership that recognized the problems it had and permitted the team to work outside the normal procurement system and IT organizations.

Relevance to DOD

We see the same promising pattern in the development of some systems in DOD. The U.S. Air Force Synchronized Air Power Management (SAPM) process is used to create an air battle plan through to a fly-out package. With the use of XML and web services

[31] We do not prescribe that documentation be ignored for DOD information systems, only that it is a low priority in the WHC solution. Documentation has its place, though it could become both more difficult and less critical as solutions become more fluid in response to continually changing user needs.

and a thoughtful design, Air Force personnel created within 12 weeks an information integration system that spanned 7 major stovepipes. As a result, the time to create a fly-out package was reduced by 60 percent (from 5 hours to 2).

What are the implications to the Defense Department and the armed forces from technical developments seen in the WHC and Air Force examples?

- The concept of interoperability needs to be rethought. Systems need not interoperate with one another. They have to produce data, but not much else.
- The creativity of the user, the soldier, sailor, airman and marine can be released to craft solutions to their need at the time they need it.
- The need for custom software is dramatically reduced.
- There is a diminished reliance on contractors.
- Tools permit the user to create environments of their choosing themselves.
- There is the opportunity to rethink basic architectures.
- There is an opportunity to avoid significant costs in procurement, operation, maintenance and training.
- There is the opportunity to question procurements still in the pipeline for their relevance, since existing systems may suffice.

The opportunities come with a price. Governance becomes a subtle issue. No longer is it an issue of control and oversight of a network, but one of participation. That participation requires an involvement and availability (both personal and regulatory) to address which constraints are relevant and which have been obsolesced by technology. We also face the issue of personnel, their skill-sets and the management of their creativity. How much should the Department and Services rely on support services and how much should be brought in-house?

The list of possibilities is open-ended. As the two examples show, there is an extraordinary chance to change a historically burdensome and frustrating situation. As DOD struggles with complex information issues at a time of extreme budget pressure, there is the real possibility that commercial technology development over the last few years can provide a path to much greater progress, with huge dividends for national security. If the costs can be squeezed out of integrating information and the value of information to users can expanded, long over-due gains in productivity in military operations and capabilities may be at hand.

The information revolution is in the process of reaching the next level. All the inventions and investments to date have created conditions in which this phenomenal new utility can enhance the performance of humans with relative ease. The fundamental reason why this particular leap in information power is now possible is simple: the creativity of users is being engaged to shape solutions. All they need is unrestricted access to information and opportunities for collaboration, which technology is now close to being able to provide.

IT has evolved from isolated computation to compatible computers linked with great difficulty to integrated networks of heterogeneous systems and now to user access to any information and any other networked user. It is only natural in this process of ever-

greater value that users themselves should begin to exercise influence and eventually dominance over how information is packaged and delivered for their use, whatever it may be. This makes it all the more important that the processes by which information needs are determined and met, in DOD as elsewhere, be redrawn with *users in charge and with extending their reach into the information world as the animating force.*

It is because of this new promise, and what it could mean for national defense, that measures to make DOD structures, processes and economics more conducive to the user's needs should not be timid. For decades, government has tried to mold IT to fit its ways of doing business. While this has had mixed results until now, it will become increasingly problematic if the demands of warfighters are to drive solutions, as they should. The reason for process reform is not that DOD cannot make do with a hodge-podge of networks—in fact, it can—but rather that strategically it cannot afford to miss the new technological, economic, and operational opportunity afforded by the creative power of information users.

IV. Reaching from the Real toward the Ideal

Introduction: Taking Stock and Looking Ahead

We are now ready to suggest a path to user-responsive information and networking in support of integrated military operations for U.S. forces, taking into account: (a) the ideal conditions suggested in Chapter 1; (b) the current conditions and efforts described in Chapter 2; and (c) the promising technological opportunities identified in Chapter 3.

Up to this point, we find DOD's effort to meet the information needs of warfighters to be a mixed picture. The networks on which warfighters depend do not provide them with either unobstructed access to whatever information may help them in battle or unbounded opportunities for collaboration with other warfighters—the ultimate standards of network responsiveness in the impending age of integrated warfare. To the extent that these two standards are not met, the promise of net-centricity and the aims of transformation cannot be realized. At the same time, user access and collaboration are precisely the values that are now being demanded of IT in the world at large. Fierce competition to furnish useful access and collaboration is already bearing fruit on the Internet, in the economy, and in personal computing.

By the same token, DOD is not tapping into the power of user creativity in fashioning information solutions for maximum effect, as illustrated in the Washington Hospital Center case in the preceding chapter. When it comes to information integration, DOD's users are not only under-privileged, they are also under-employed. The reason to back up the needs of users with economic power, as we recommend, is not only to be more responsive to their demands but also to engage them in developing more elegant and useful information solutions. In this sense, the way the Internet is continuously reshaped and enhanced by users—and by providers who are keenly attentive to them—is at least as instructive for DOD as its technical attributes. Once again, DOD is in danger of missing this wave and then having to swim after it.

Notwithstanding its tardiness in addressing user needs and employing user creativity, DOD is making significant progress in improving C4 infrastructure. This progress is the result of: (a) the belief of its civilian and military leaders that networking helps U.S. forces perform more effectively and is essential to national military strategy; and (b) the increasingly insistent demands of warfighters for improved network-based awareness and collaboration in order to face real needs and dangers in current operations. These same two actors—institutional leaders and operational users—are the key to achieving greater success, and it is fair to say that neither one is satisfied that DOD is exploiting as effectively as it should be the continuing, wider revolution in information networking.

Looking ahead, substantially broader and faster progress is possible thanks to: (a) recent user-led technological advances; (b) the acceptance of the operational pay-off of both jointness and networking by more and more of the U.S. military establishment (owing, in part, to the lessons of Afghanistan and Iraq); and (c) commitments already made to enhanced network infrastructure and services (e.g., GIG-BE, TSAT, JTRS, NCES, and

GIG-IA). While not necessarily the truest measure of commitment or reliable indicator of future progress, it is noteworthy that investment in information—communications and intelligence—has gone up by 50 percent between 2001 and 2005, after having been essentially flat throughout the 1990s.[32]

Yet, there remain large obstacles that resources alone cannot overcome. The most serious are: (a) DOD's own processes for setting requirements, allocating resources, and managing investment; and (b) within these processes, the centrality of the separate armed services in meeting operational information needs (under their Title 10 responsibility to "equip" forces). DOD processes are an obstacle because they are slow, structured, regulated, and predicated on predictability, whereas information systems and services markets shift rapidly, bear fruit continuously, chafe at control, and are largely unpredictable. The centrality of the individual services is an obstacle because their choices place insufficient value on integrated joint operations and requisite C4.

These boulders must be removed from the path if broader and faster progress is to be made toward networks that respond to joint warfighters' information needs, and thus to the strategic imperative of integrated warfare. With congressional support, their removal is within DOD's power. Yet, both go to the heart of how DOD does business and are based on ingrained practices, regulations and laws—e.g., the Federal Acquisition Regulation (FAR), the Competition in Contracting Act (CICA), and Title 10—that span the careers of practically everyone in today's military. Changing processes and redistributing authority is never easy.

Leaders, Users, and Providers

With leaders and users as the chief beneficiaries of change, the organizational formula for progress is a blend of targeted *top-down* intervention and unchained *user-in* power:

- Top-down intervention must be supplied by two key DOD corporate officers who must represent the equities of national defense strategy: the CEO (namely, the Secretary) and the CIO.
- User-in power must be defined by the evolving needs of warfighters at every level and be transmitted to information network providers via joint commands, namely COCOMs and JFCOM.

Selective—precision-guided—corporate intervention should concentrate on, and be limited to, setting conditions so that user-in power can grow and assert itself. In particular, re-drawing processes and authorities in information requirements-setting, resource-allocation, and acquisition can only be accomplished by SECDEF. As the CEO and CIO effect reform, user-in power will gain purchase, allowing top-down intervention to recede. In these new conditions, the information needs of integrated operations, as well as the networking requirements implied by those needs, will be set by joint commands on behalf of warfighters. Even then, the CIO must remain an active participant to ensure that the equities of national defense strategy are served.

[32]National Defense Budget Estimates for FY 2006, Office of the Under Secretary of Defense (Comptroller), April 2005.

In such a new institutional steady-state, DOD will be better able to drink from the fast-moving stream of user-driven information technology and markets, making it more responsive to the needs of warfighters and to the goal of integrated operations. And by shortening the distance and time that separate operational need and technological innovation, the cost of IT for DOD should begin to decline at something like the rate of decline from which the rest of the IT market has benefited in recent decades.

In understanding the need for such a shift, as well as in making it work, the distinction between networks and the information they deliver is critical. It is the integration of information instead of the interoperability of networks that matters to warfighters in joint operations. If the former can be increased without the latter, fine. Warfighters should not have to concern themselves with *how* networks permit awareness and collaboration. What happens behind their screens is of importance only as it affects their ability to get valued information and critical help from other warfighters in battle.

Data networks—like the telephone network and the electricity distribution system—essentially provide feeds of information that users can employ. To say that networked information is becoming, or should become, a "utility" is not to denigrate its importance but to recognize that its achievements to date now permit a shift to an even more productive plane, in which users exploit information access and the capacity to collaborate with unprecedented ease and effect. Analogous to other distribution systems, the more robust, reliable, ubiquitous and accessible data networks become, and the more integrated is the information that they supply, the less noteworthy are their equipment, features, media, and devices to the user.

This distinction is important because it means that users can be given dominance, economically and organizationally, over both information itself and the nature of solutions to their information needs, which will in turn guide the design, creation, and operation of networks by those responsible for providing the infrastructure and feed. Users can exert control over information solutions while being indifferent to network capabilities and technological complexities.[33] The distinction also helps clarify the true identity of users and providers: warfighters under the joint combatant commands are *information users*, and others in the system, including the military services, are *network providers*.

As the previous chapter describes, new advances in software are permitting users to explore, pull, process, and exploit the information on installed networks and to shape the capabilities of new ones. Such capabilities are very relevant to DOD for several reasons:

- they yield solutions that serve users;
- they offer quick and continuing enhancement;
- they are flexible;
- they offer resourceful use of legacy systems; and
- they reduce integration difficulties and costs.

[33] There is overwhelming evidence that proficiency in using information systems requires little or no understanding of how they work or how they are constructed.

But this approach will only work for DOD and U.S. forces if users are given the power to make it work. Making warfighters' needs for awareness and collaboration predominant will tend to drive solutions, services and systems toward delivering information integration. In the ideal state, those needs are expressed through the way users demand and use information, not through central planning. But DOD does not and cannot provide an ideal, market-based setting for the expression of user needs and the free-wheeling exploitation of information technology in response to those needs. How, then, should DOD proceed to meet the growing information demands of users with the growing array of technologies designed to do just that?

Conditions for Progress

Getting the Network to the User

While emerging technology allows the user community to fashion its own information solutions, work must still be done on military networks themselves before warfighters can hope to have the unobstructed access and unbounded collaboration required for effective integrated operations. In particular, providing for the tactical end-user—the moving warfighter, on or behind the front line, in a remote part of the world, taking and giving fire—lags behind progress in providing for senior commanders and their staffs.[34] The military's equivalent of the boardroom has had precedence over its shop floor. For that matter, the leverage of military end-users in extracting information and shaping solutions trails that of many non-military end-users, including the active Internet user and the average traveler.

The problem of the deprived military end-user is also related to the difficulty of extending enough bandwidth to support operations beyond the United States. Ironically, if unsurprisingly, DOD's networks are far more robust where wars are not fought (at home) than where they are fought (away). In addition, reconciling the ideals of unobstructed access and unbounded collaboration with the need for information security remains a major technical and architectural challenge. These and other military network shortcomings are in part a consequence of:

- insufficient definition, communication, and resourcing of the data needs of the common joint warfighter—the neglected shop floor;
- the fact that DOD's processes do not permit continuous, flexible, and timely uptake of new—better, cheaper, user-oriented—information technology;
- the impeded and imperfect flow of technology and solutions to the military domain from the huge, fast, global, and innovative IT market and industry.

Remove the two obstacles mentioned earlier, and these deficiencies can be remedied.

Make Joint Integration Priority Number One

If broader and faster progress is to be achieved on both the information and network levels, setting priorities will be important. The reference point for priorities is conceptually simple: Whatever contributes the most to operational integration for joint warfighting—including the information integration (shared awareness and joint

[34] Maryann Lawlor, "Iraqi Communications Transition From Tactical to Practical: Military builds foundation for the Future," *SIGNAL Magazine* (November 2004)

collaboration) on which operational integration depends—should be the highest priority in technology exploration and network investment. If priorities are set this way, it may be possible to make dramatic progress toward meeting the information demands of integrated warfare in a matter of years, even if it takes decades to bring military-wide networking up to the same standard.

For meeting the high-priority information needs of operational integration, especially for joint C4, we will make some radical suggestions regarding DOD processes and authorities. For other C4 needs, reform can be less urgent and radical. It may well be that most C4 can, for now, be left to the services functioning within established DOD processes. After all, only a fraction of forces and operations are, at present, affected by joint integration. Thus, realignment of processes, authorities, and allocation of resources need not be comprehensive but instead can be concentrated on meeting information and network needs that affect integration.

In practice, separating those information needs that enable forces to conduct integrated operations from those that do not is not easy. If the former needs are to be met in a different way than the latter needs—in essence, the former by the joint commands and the latter by the services—a dividing line must be drawn. This is a natural corporate function, and should be performed by the CIO. Where there is ambiguity about whether jointness is essential, there is nothing wrong with cooperation between the joint community and a service.

Throughout the effort to make information and networks more joint and more user-responsive, strategic perspective must not be lost. Indeed, the reason why IT for integration should, in general, have priority over IT for other purposes is strategic. Given its global security interests and responsibilities, the United States will face a diverse set of state and non-state adversaries—typically asymmetric but determined, even fanatical. Because these adversaries do not bother with the niceties of democratic accountability and regulation, they are not saddled with the likes of DOD's PPBE, CICA, and the FAR. While they lack the resources of the U.S. military, they can "cycle" as rapidly and continuously as information technology and markets do—and much faster than we can.

Consider the transformation of al Qaeda within a couple of years of the defeat at Tora Bora. Consider the mutation of the Iraqi insurgency within a year of the capture of Saddam Hussein. In both cases, increasingly distributed structures have made ingenious use of largely public information infrastructures. There are indications that the relationship between China's burgeoning IT sector and the Peoples Liberation Army (PLA) is closer than the rather distant one between American IT firms and DOD, which means that technology may be able to move relatively swiftly from China's economy to its military.[35] And since China's economy is an integral part of the world economy, including in IT, the ability of the PLA to extract militarily beneficial technological innovations from the global IT pool should not be discounted.

[35] Robert C. Fonow, "Beyond the Mainland: Chinese Telecommunications Expansion" Defense Horizon (Center for Technology and National Security Policy at the National Defense University, Ft. McNair, Washington, DC) July, 2003.

This strategic perspective underscores the compelling need for U.S. forces to be able to conduct integrated operations. While the general virtues of jointness need no elaboration here, it is worth noting why deeply integrated operations are especially important in the current security environment:

- First, because contingencies and circumstances encountered in any given contingency are unpredictable and may be unfamiliar, there is benefit in having maximum flexibility in the way forces are combined and used. As we saw in the teaming of SOF, Navy Air, and USAF long-range strike in Afghanistan, only the ability to integrate—ad hoc, not merely pre-planned—will provide such unprecedented flexibility.
- Second, the capabilities and tactics of current and future adversaries demand deep operational integration on our side. On the one hand, integration can counter the agility and elusiveness of irregular forces; on the other, it can increase lethality and survivability against more traditional enemies that are incapable of integrated operations.
- Third, only through integration is it possible to derive maximum advantage out of two other IT-based capabilities: precision and shared awareness.

For these strategic reasons, the U.S. military needs to exploit IT in order to achieve joint operational integration more quickly. Moreover, in this complex and shifting security environment, U.S. warfighters must be able to think, decide, and act faster. Thus, in terms of both strategy and operations, time is precious, and speed is paramount. Just as the think-decide-act cycle must be reduced, the pace of exploiting IT must be accelerated. DOD is a complex, "legacy" bureaucracy, accountable for vast public monies and governed by a federal procurement regulatory regime. It excels in control, not speed. DOD must shift from a paradigm of control to one of speed if it is to exploit IT.

Vision Matters

The quest for responsive information and networks must be guided by a clear and agreed vision that transcends personalities (e.g., the incumbent Secretary) and links the strategic aims of leaders with the operational demands of users. For the strategic reasons just mentioned, that vision is one of *deeply integrated and highly fluid operations* supported, and not constrained, by the availability and quality of information or the capacity and functionality of networks. This does not mean that all units would function this way all the time in all operations. However, in no cases should they be prevented from doing so by the limitations of information and networks. We simply do not know what paths of information access and what collaboration will be important in the future. Not that long ago, the idea of a cruise-missile-bearing submarine acting in concert with a Marine reconnaissance unit and tactical-strike aircraft would have seemed far-fetched.

Because of the operational and strategic importance of this vision, every process reform and IT investment must be traceable to and measured against it. Even if the vision seems far beyond current reach, its importance should motivate progress and its clarity should inform metrics for reform and investments to achieve that progress.

At the same time, as just noted, deep integration is not of uniform relevance in all aspects of military operations. It is more important to achieve the vision, or at least to achieve it sooner, for some missions than others. For example, close air support (CAS) depends vitally on *joint* shared awareness and collaboration, whereas anti-submarine warfare (ASW) depends on shared awareness and collaboration only among *maritime* platforms (for now). While the Navy can address information needs for ASW within its own operating concepts and priorities, the information needs to support CAS must be addressed jointly. Current processes and service-centricity may be fine for the former, but not for the latter.

This vision of deep operational integration encompasses the two basic information user needs of access and collaboration. The need for warfighter information access is self-evident—the fuller, clearer, timelier, and more shared the "operating picture," the better. The need for warfighter-to-warfighter collaboration—horizontal, regardless of service—is at least as important as awareness in shaping network responsiveness. If joint operations are no more than coordinated service actions with programmed episodes of cross-service interaction, satisfying C4 needs is much easier than if joint operations are deeply unified and involve self-organized ad hoc teaming across service lines. The evolving strategic situation makes deep and fluid integration essential, and the emerging user-pull information technologies make it possible, assuming DOD can harness them.

In sum, deep and fluid operational integration depends on unobstructed access and unbounded warfighter-to-warfighter collaboration, making these two basic user needs the alpha and omega of the pursuit—the objectives, programs, criteria, and metrics—of network responsiveness.

Formula for Progress

Obviously, fulfilling the information and network demands implied by the vision of deep and fluid operational integration will be challenging. New user-responsive technologies are well suited to meet this challenge. The key will be to institute processes within DOD in which user demands and technological possibilities are closely and strongly linked, rather than separated by bureaucratic filters, well-meant staffing, planning cycles, program-management structures, and constant top-down interference. Yet, good governance is needed to create and tend this user-technology link. Thus, the formula for progress has three key factors:

- Technology: What are the possibilities for enhancing user-reach?
- Processes: How can user-reach be enhanced, now and perpetually?
- Governance: What conditions must be set, by whom, to improve processes and exploit technological possibilities?

Keeping in mind that not all military C4 and IT bear directly on the challenge of enabling deep and fluid integrated operations, priority should be placed on applying this formula to those that do, with the expectation that C4 and IT for other (e.g., intra-service) requirements can be provided by business-as-usual, at least for now.

Technology

While IT continues to surge on many fronts, the most momentous developments at present are those that can increase both the benefits and the influence of end-users. This is illustrated in the preceding chapter, but it is also apparent to all who use the Internet. The logic behind these developments is quite simple: end-users know best what information will benefit them; therefore, giving them greater power in pulling information and in determining information solutions is the surest way to maximize their benefit (and the ultimate success of the provider). Because of the rewards they offer in the economy at large and the wonders of creative engineering, these technologies will develop rapidly—indeed, they already are developing rapidly because they enable people to make greater and faster use of the Internet.

The previous chapter explained how new tools permit users not only to gain access to disparate information systems but also to create information environments of their choosing. This opens up tantalizing opportunities for DOD:

- To finesse the problem of poor network interoperability;
- To unleash the creativity of users to craft living solutions to changing needs;
- To reduce the need for custom software;
- To diminish dependence on systems integration (and contractors);
- To reduce costs in procurement, operation, maintenance and training;
- To compress time between identifying an information need and having a solution.

With the goal of warfighter responsiveness in mind, the most important of such developments is the advent of methods and systems that facilitate *user-reach in heterogeneous network environments.* Such approaches as "meta-data tagging", wrapping of "info atoms," and "directories" provide users access to networks that may lack connectivity to one another. They thus provide network-information integration without needing network-system integration.[36] They are taking hold in the wider (non-military) world, are of growing interest to DOD users and providers of information systems, and are key to some new DOD network capabilities, especially NCES.

This development raises some interesting questions: Has the network-interoperability problem been overtaken by user-pull technology, at least in theory? Is there a future for legacy systems? Given the leverage of this concept, both in improving operational responsiveness and in making use of disparate existing networks, are the enabling technologies being given enough emphasis by DOD? What applications are working within and outside of defense that should be expanded and accelerated? Are the existing requirements-setting, resource-allocation, and acquisition processes conducive to an ambitious approach to user-pull solutions and technologies? If not, how should they be modified, within the constraints of sound stewardship of public resources?

Although recognizing the potential—after all, DOD employees are also Internet users—DOD is in danger of not fully and quickly availing itself and its troops of the best that IT

[36] Networks do not need applications interoperability because they transmit universally understandable data (with common syntax and common semantics, by agreement), thanks to Internet Protocol and post-pull standards like http and html.

has to offer on the particular challenge of user-reach. The timelines of technology are a fraction of the timelines of government budgeting and acquisition. If NCES is "procured" in the same programmatic manner as other DOD "programs"—and we do not know that this will necessarily be the case—the U.S. military will once again be a straggler in benefiting from IT breakthroughs, and it could find it hard to refresh this bundle of user-support services with the inevitable flood of ensuing enhancements. More generally, unless processes are overhauled, at least for those information capabilities that support joint integration, DOD will be behind the technology, behind non-military organizations in using it, and behind the needs of joint warfighters. Ironically, it may also disadvantage U.S. fighters against terrorists who rely increasingly on user-reach through the Internet and thus benefit more or less directly from technologies and innovations in the global IT pool and information realm.

Unlike legacy information systems, the design of new information systems can be derived from joint-integrated operational needs and optimized to support user-reach methods. At the same time, legacy systems could be less of an obstacle to operational integration than previously thought, and they have the cost-benefit advantage of having been mostly paid for. While there may be other reasons to replace legacy systems, software advances seem to be overcoming the problems of access and connectivity. Allocation of resources between investment in new systems and utilization of legacy systems should be made according to the guiding strategic-operational-informational criteria of unobstructed access and unbounded collaboration—and, of course, cost. The right question is: Where will the next dollar do the most good relative to integration?

Despite exciting technological advances, the practical difficulty of providing user-reach capabilities to the warfighter—in particular, the tactical warfighter—should not be underestimated. Actual battlefield operational conditions and information needs are typically complex, unfamiliar, and changing—unlike, say, checking on airline fares or retrieving medical data. Because time is critical, reliance on browsing is no panacea. For this reason, DOD should look especially at advances, including non-military applications, that address urgency. Also, security is bound to be a concern if access is to be provided on demand, and with minimal delay, to users based on need as they see it.

Given such technical and architectural challenges, it will take no less than the commitment of top IT industry talent to apply these user-responsive technologies to military networks, working directly or through defense systems integrators. Although the military's urgency and security problems are especially severe, solving them will require the kind of innovation that has propelled the Internet. In this regard, DOD processes can do harm in two ways: delaying uptake; and de-motivating IT firms from committing to develop solutions, preferring instead to leave the hassles of DOD acquisition and contracting to defense systems integrators. Conversely, an important collateral benefit of IT/C4 acquisition reform (described below) is that it would attract technology firms to help DOD solve the problem.

With progress in open systems and, more recently, user-pull technologies and solutions, the role of defense systems integrators in military IT and network development and

acquisition may become less critical. The need for massive technical integration and custom software to allow systems to work together may diminish. For now, defense firms provide important understanding of users, missions, and the acquisition environment—though, as we argue below, the environment should be made more hospitable to the firms that generate IT, ideas, and solutions in the market at large.

Lastly, DOD should pursue technologies that can make information easier to reach and share during urgent and complex operations. Realistic voice-activated word processing, low-cost video teleconferencing, and mobile IP could improve user-responsiveness and increase use of networking. In sum, priority should be given to information and network technologies that extend bandwidth and service to warfighters, give them ways to pull from disparate networks, support shared awareness and collaboration, and make information access easy and quick for people who are, lest we forget, busy fighting wars.

Processes

Similar to creating other defense capabilities, providing users with responsive information networks requires (a) specifying needs, (b) allocating resources toward meeting those needs, and (c) investing in research, development, and procurement in systems and services that deliver the capabilities. That, however, is where the similarity ends. The technologies associated with information systems and services are propelled by vast, fluid, and largely unmanageable markets and industries, unlike most of the technologies associated with such military equipment as missiles, tanks, submarines, and combat aircraft. With some exceptions (notably, network security), DOD has slight influence in these markets and underlying technologies when compared, for example, to the influence of the Internet's billion or more users. Consequently, DOD must participate in these markets *as they are*, not as DOD might want them to conform to its standard processes and rhythms.

As a thought experiment, imagine being a private, but patriotic, consultant with the chance to design how a potential adversary of the United States goes about trying to exploit IT for military purposes. You would not want that adversary to conduct integrated operations, to be able to field the latest solutions that enhance awareness and collaboration, to update those solutions continuously, or to benefit from innovations in the market at large. So you might design a system that is rigid, centrally planned and controlled, able to buy only every so often and not replace until years or decades later, influenced by parochial interests that do not see the virtues of integration, and subject to industrial politics. You have just designed DOD's system for identifying C4 needs and meeting those needs with IT. (Another illuminating, not to say entertaining, thought experiment is to consider what life would be like if building the Internet had been entrusted to the government operating under the FAR! It might still be drafting the request for proposals.)

DOD's processes are too inflexible, structured, slow, and regulated to exploit information network markets and technologies. The reasons why these processes are what they are—e.g., fair competition, congressional accountability, stewardship of public resources—

cannot be dismissed. Any changes must, and we think can, respect these underlying principles.

Let's look at each of the three main processes and how they might be improved while remaining true to the principles just endorsed:

1. Specifying Needs

Information networks exist largely to support C4. With the pursuit of operational integration, C4 is increasingly a joint function. It follows that information and network requirements should flow from joint operating needs, such as those associated with joint-force "battle management" and spontaneous cross-service tactical teaming.

Efforts to identify the capabilities required for joint operating concepts are already underway. The new joint force planning system, JCIDS, is meant to define force requirements for those missions that are best performed jointly. However, JCIDS is still a bureaucratic and structured process, as opposed to an economic and continuous one. It is important to receive, analyze, and answer user demands (e.g., for network features and functions) without bureaucratic interference or interpretation. For now, refining JCIDS appears to be the best option; but it will have to be augmented by more direct, market-like, and continuous signaling of user needs. For example, the joint C4 needs identified in JCIDS could be compared to the specific needs the COCOMs are rushing to meet.

Collating, interpreting, and prioritizing needs—especially different ones from different COCOMs—will require some sort of broker among the COCOMs that can also be their agent. The advantages of having JFCOM fulfill that function are several:

- Its *raison d'être* is to develop and generate capabilities for integrated operations;
- It is already responsible for providing joint C4 to COCOMs;
- Its perspective is both joint and global;
- Its time-frame is both near- and (unlike the COCOMs) long-term.

As noted, many C4 requirements will be unrelated to integrated operations. As the separate services identify and go about meeting such requirements, they should at least be screened by JFCOM and certified by the CIO to ensure compatibility with joint C4 architecture and standards.

2. Allocating Resources

One of the most consequential anomalies in the way DOD attempts to exploit information technology is that its users have no economic power. Any measure to engender market-like forces should be helpful. Within DOD, this would mean allocating resources to the joint community to acquire those information solutions and networks that are needed to integrate operations, based on users' needs *as users see them*.

Presently, nearly all investment resources, including those for information systems, are allocated to the separate services. The services are oriented toward enhancing capabilities by equipping forces with platforms, weapons, and sensors, rather than enabling integrated operations, shared awareness, and collaboration via joint C4. It is unrealistic, even unreasonable, to expect a service to give *higher* priority to how its forces will interact

with those of other services than to maximizing the capabilities of its forces. As long as all or nearly all money is allocated to the separate services for C4, do not expect joint C4 and the networks that support it to be a high priority; do not expect user-access across service lines to be a high priority; and do not expect the means to enable inter-service collaboration in battle to be a priority. Insofar as a service can be expected to see the merit in operational integration, it is more likely to see it through an intra-service than an inter-service lens. The clearest proof of this are the current major efforts of each of the services, described in Chapter 2, to develop the means for forces across that service to interact, with jointness a secondary consideration at best.

The way the joint commands are allocated resources for C4 to support integrated operations should fit with the requirements-setting and brokering functions mentioned above. Allocating investment resources to regional COCOMs should be restricted to emergency needs, e.g., to support imminent and ongoing operations. In the main, JFCOM should be allocated the resources for joint C4 investment. Of course, JFCOM could in turn mandate and fund one or another service as agent for requirements relevant especially to it—with the understanding that those funds are not the service's to reprogram. For example, JFCOM will want to be sure that the Navy's integrated network (FORCENET) will support joint expeditionary operations from sea bases. After having set the joint requirement and secured the requisite funding to make this so, JFCOM could make the Navy responsible for enabling C4 for all forces using this maritime platform.

Even with the allocation of funding to JFCOM for all C4 related to integrated operations, it may still not be confident that the importance of its needs will be recognized within the normal DOD PPBE system. Defense resource allocation depends heavily, as it should, on the expected marginal operational impact of having a certain capability. Will the next dollar contribute more to winning battles if invested in, say, a new air-to-ground missile or instead in a new joint-C4 network feature? Normally, the estimate of marginal impact depends on certified computer-based models of military operations. In competition for dollars, C4 systems and networks tend to fare badly against weapons, platforms and sensors, mainly because it is harder to measure their effects (given the importance of cognitive variables). Compared to other warfighting systems, the expected return on tax-payers' investment in C4 is less easily shown.

How much of the DOD budget is allocated to JFCOM for joint C4 should be settled through PPBE. However, recognizing both the strategic importance of integrated operations and the difficulty of modeling and quantifying the contribution of information and networks to the outcome of operations, this is one way in which top-down intervention could be essential. In the early years of corporate IT investment, CEOs, CIOs, and CFOs believed but could not prove that networks would pay dividends in labor productivity, operating efficiency, cost structure, competitive position, and eventually on the profit line. Their convictions led to strategic investments above and beyond what their various lines of business could justify. (The impressive IT-based productivity gains in the American economy have since validated their instincts.) At the same time, injection of funds from the Secretary should not go on indefinitely. In time, either new models will

reveal the expected operational impact of C4 enhancements or user demand will prevail over model-based resource allocation.

3. Investing

Once again, the DOD acquisition process is oriented toward procurements of distinct and durable "things." It is also geared toward things that are unique to the military, which tend to be distinct and durable. The process is complex, structured, controlled, and slow. It is managed in project and program blocks and calendars that have boundaries, beginnings, and ends—parameters that do not apply naturally to networking capabilities and investments. More than the requirements-setting and resource-allocation processes, the investment process is badly—perhaps irremediably—out of tune with information technology and markets, which turn over at a much higher rate than military-unique technology and markets.

This problem is widely recognized within the defense establishment. The acquisition process is already being compromised in the face of these forces. As described in Chapter 2, organizations of DOD can engage in "rapid acquisition" to get network equipment for urgent use. Exceptions are being made to provide information systems to augment deploying and operating units' networks. This method serves as a pressure-reduction valve; it is inadequate and should not be mistaken for reform.

Urgency is not the only reason to create a streamlined acquisition process for joint C4. The other reason is that established acquisition decision and management approaches work at cross purposes with fluid information technology and markets. Even information capabilities that are not needed urgently should, nevertheless, be acquired in a way that enables DOD to buy from fast and continuous IT markets.

To be clear, military users need not replace their information systems whenever the market and/or technology advances. Some improvements, e.g., software releases, can be incorporated gracefully. Others can await a natural and economic cycle for upgrading. Commercial customers do not, obviously, replace their systems just because something better is "out there," any more than the typical home replaces its computer or upgrades its Internet connection annually. The key for customers—persons, firms, or military forces—is to be able to advance as frequently and as quickly as they choose. That way, if some technology could improve their work or lives, they can have it easily and without delay, which is especially important in competitive domains.

Many of the companies that generate information technology, systems and services recoil from DOD acquisition processes (and slim profit margins). Absent a different acquisition process, do not expect many of the companies that create new network technologies to pursue defense business more than opportunistically and/or as sub-contractors to defense systems integrators. Even if one or several do, this hardly assures sufficient competition and flow of innovation from the national (and global) IT economy to the defense economy.

Keeping in mind the centrality of joint integration in U.S. defense strategy, the need to extract value from IT industry, and the aversion of that industry to bureaucracy and control, DOD's C4 acquisition process should differ sharply from its regular process:

- First, the C4 acquisition process should stress continuous acquisition, flexible funding streams within agreed scope, greater customer latitude regarding competition, and easing of milestone and change-control protocols.[37]
- Second, customers for joint information solutions and networks should be joint organizations that are in a position to appreciate and represent needs of warfighters in integrated operations.
- Third, the process must be designed so that it is not incompatible with the business models and return-on-equity standards of the IT industry—i.e., shorter timelines, commercial risk-reward equations, less onerous administration.
- Fourth, because they tend to be inflexible and not conducive to competition, huge structured procurement programs should be used not out of convenience for acquiring information solutions but on those rare occasions when they are essential.

Making every COCOM an investor could create new stove-piping based on regional idiosyncrasies, connectivity problems (given that military units do not always operate under the same COCOM), and a bias toward short-term needs. Because JFCOM is already responsible for providing the COCOMs with joint capabilities—of which none is more critical than C4—it is the logical organization to serve as the customer. There is also logic in turning to the same organization that would serve as global broker for requirements and manager of resources for joint C4, as we suggest.

There could be doubts about concentrating this much power in a single command. Some might consider it unwise to place total reliance on one organization to make and manage investment in all C4 required for joint operations. We disagree: in this case, monopsony would not only improve coherence and connectivity but also give DOD's warfighting IT users more power in the market. There may also be concern that giving JFCOM the authority and resources to set and meet joint C4 requirements would deny a voice to others in the military establishment—for example, the service chiefs. One possibility would be to place responsibility with the Joint Staff, for example, which would use JCIDS to develop a common view of joint C4 requirements for approval by the JCS (via the JROC). Such an approach would be a straight-line extension of traditional and current practice, designed to "bring the services along." Again, we are wary of relying on anything this close to the bureaucratic status quo, which does not work. The central role of JFCOM in C4 requirements-setting, resource allocation, and acquisition would concentrate a lot of power. However, it is precisely the concentration and enhancement of user-power that is needed. Moreover, effective governance of DOD's exploitation of IT should ensure that such concentrated user-power is accountable.

Thus, in the interest of meeting the need for information solutions that favor user-access and collaboration in integrated operations, the processes of requirement-setting, funding,

[37] This, of course, raises the problem of how to acquire information solutions that are embedded in other systems, such as combat aircraft.

and investment should be reformed as a package to facilitate DOD exploitation of new technology and innovations that are working in the economy at large. The key to re-engineering all three processes is to enhance user-power in a way that both satisfies current joint-operational demands and promotes the goals of access and collaboration. JFCOM should set requirements based on a combination of current COCOM needs and the long-term implications of integrated joint warfare. This same alliance of JFCOM and COCOMs should be allocated resources so that they can back up their needs with economic power that does not compete with service-centered equipment. Resource allocation to support joint networking should, as required, receive top-down help, given the strategic equities in fostering integrated operations.

Such changes need not run afoul of the core principles of fairness, transparency, and accountability in government procurement. Indeed, acquisition reform for joint information solutions would *increase* competition significantly—by attracting IT firms into the defense market—and might even enable DOD to benefit more than it has to date from declining IT costs. Thus, in the interest of better defense at less cost by exploiting excellence in IT, some adaptation of the FAR and CICA would be required, as would some shaving of Title 10 responsibilities of the services.

At the same time, each of the services may continue to address those C4 needs that they consider essential to the forces they are expected to provide. They would have to assess needs, weigh C4 investment against other service priorities, seek funding, and manage investment. The boundary between JFCOM responsibility and service responsibility would be set according to those missions that are deemed to require cross-service integration, shared awareness, and collaboration, with the CIO as the final arbiter. Of course, JFCOM cooperation with one or another service could be the ideal approach in cases where the information used and/or generated by a new weapon system (e.g., the F-35) must be integrated with joint networks.

Governance

Chapter 2 details how assiduously DOD management is striving to meet information needs and foster joint integration. However, we are convinced of the need for better aligned efforts to promote user-responsive networks and to support the joint warfighter. To this end, it is essential to be clear about the fundamental responsibilities of key players in governance. We are convinced of the value of a troika with complementary responsibilities (rather than some czar).

1. SECDEF—the Strategic Stakeholder

SECDEF has three indispensable functions in advancing the use of information by U.S. forces—rhetoric, reform, and resources. The first is to proclaim the objectives of unobstructed access and unbounded collaboration for warfighters, in support of the vision of deep operational integration unconstrained by network capabilities. In addition to using his bully pulpit, SECDEF must see to it that these goals are institutionalized and used practically as the points of reference to measure progress and investment returns. While we caution against the sort of detailed bureaucratic action plans, which rarely help in the free-form world of information, it could be useful for SECDEF to set annual or

biennial targets for progress in user access and collaboration. Metrics could be based on relevant network capabilities. Better yet, they could rely on user polling—the military version of customer-satisfaction surveys.

The second function of SECDEF is to prepare the necessary organizational conditions for the achievement of the grand objectives: shifting authorities, aligning resources with these authorities, and reforming processes to empower users. With congressional support, SECDEF (and only SECDEF) can establish the role of JFCOM in setting and satisfying information and network demands to support joint integrated operations. In so doing, SECDEF would be putting user needs for access and collaboration foremost.

Lastly, SECDEF must ensure that adequate investment is made in user-responsive networks, notwithstanding strong competition from weapons, platforms, sensors and other equipment. To some extent, ending dependence on the services to provide C4 for integrated operations should reduce the problem of platform, weapon, and other investment demands eating into funds otherwise available for C4. Still, it may be necessary to use "corporate" investment in light of the importance of C4 and the difficulty of getting the PPBS to recognize that importance.

2. DOD's CIO—the Vicar

The CIO should have two masters—SECDEF and the user—and should be responsible for connecting and satisfying the strategic demands of the former and the operational demands of the latter. The CIO must see to it that the requirements, resource-allocation, acquisition, and standards review processes are advancing the SECDEF's declared objectives of unobstructed access and unbounded collaboration. The CIO could be measured by whether adequate progress is being made toward those objectives in the time-frame set by SECDEF. In turn, the CIO should measure the military's progress. To facilitate this, the service CIOs should report both to their service chiefs and to the DOD CIO.

The position of the CIO relative to the other DOD "corporate officers" (i.e., undersecretaries) is also important. The CIO must have influence with the Comptroller to make sure that investment-resource allocation does not neglect joint C4, given the services' predilection for buying weapons and platforms. Similarly, the CIO and the Undersecretary for Policy must try to integrate information strategy and overall defense strategy, given the importance of the former for the latter. Lastly, the CIO and the Undersecretary for Acquisition, Technology, and Logistics must develop and manage an acquisition system that is tailored to satisfy joint C4 needs and to keep pace with wider information technology and markets.

The CIO's responsibilities subsume but extend beyond overseeing the development and support network infrastructure. Double-hatting of the CIO and the Assistant Secretary for NII (described in Chapter 2), which is the case today, risks creating at least the perception if not the reality that the CIO is little more than the senior network official. Because the CIO's responsibilities are broader—in essence, ensuring the effectiveness of *all* information flow within DOD and among U.S. forces—it might be better to have the

senior official overseeing network infrastructure report to the CIO (i.e., two hats on two heads). If the CIO were to be a DOD under secretary, as the responsibilities described here imply, the position could subsume intelligence as well, on the grounds that intelligence is a subset of the total information challenge. [38]

DISA is the technical organization that enables the CIO to meet these responsibilities. It develops and maintains global joint C4 systems at the CIO's direction. Just as the CIO's responsibilities should be expanded, so should DISA's role and capabilities.

Using DISA, the CIO is responsible for providing the military with the infrastructure, expertise, and support services to translate operational requirements into networking requirements and to manage networks. Similarly, in carrying out its acquisition function, JFCOM should rely on DISA not only for long-haul networks, e.g., GIG-BE and TSAT, but also for joint tactical C4. Under the CIO, DISA should be the authoritative source for technical standards, specifications, and assessments. This will require explicit organizational change and also augmentation in DISA capabilities beyond those associated with backbone networking. No other organization, civilian or military, currently has DISA's technical capabilities; rather than proliferating technical capacity as DOD and the military become more network-dependent, arrangements should be in place to provide any and all with access to DISA. This could require shift of some technical capabilities currently scattered around DOD into DISA.

3. JFCOM—the Customer-in-Chief

JFCOM is already principally responsible for joint force integration, including the responsiveness of networks to the objectives of access and collaboration. In this capacity, JFCOM is responsible for consolidating and harmonizing network requirements of the COCOMs and for ensuring that investments in network systems meet connectivity criteria. JFCOM has recently been given limited authority to procure C4 systems. This would be changed to line authority for ensuring that COCOMs' current and future information and network needs are met. Logic suggests that JFCOM would also be responsible for meeting the C4 requirements of STRATCOM, which is the provider of global C4 bandwidth and service for the COCOMs.

As already discussed, the responsibilities of JFCOM should be expanded to include final military authority in setting C4 requirements; the manager of resources allocated for C4; and the principal customer of network research, development, and procurement. Given these roles, JFCOM would be the counterpart of the CIO within the military user community and the agent of the COCOMs for networking. In DOD's information "market", JFCOM would concentrate on and perform the demand function. Its technical support, again, should come from DISA.

To be effective, JFCOM would have to have decision authority not only in DOD business processes but also vis-à-vis the COCOMs. Rather than merely coordinating and voicing the COCOMs' C4 needs, as the Joint Staff is currently supposed to do, JFCOM should

[38] By way of comparison, corporate CIOs are often among the half-dozen or so top officers, along with CEO, COO, CFO, and major business-line heads.

synthesize their joint C4 needs, analyze future needs the COCOMs may not know of, and then decide what is needed, subject to civilian (i.e., CIO) oversight.

This is a tall order for JFCOM. Some might argue that such a role would spread JFCOM too thin. However, setting and meeting requirements for C4 is the most important of JFCOM's responsibilities, because joint operational integration depends vitally on shared awareness and collaboration. Indeed, the responsibilities suggested here go to the heart of why it was deemed necessary to create JFCOM in the 1990s.

In sum, this governance troika would thus encompass (a) the strategic interest in furthering integrated operations (SECDEF); (b) the demand for capabilities to meet user needs and to allow unobstructed access and unbounded collaboration (JFCOM); and (c) stewardship of these two interests in DOD's business processes (CIO). Moreover, it would include strong civil-military teamwork (in CIO and JFCOM) and strong, common technical, professional support to both from DISA (which should support all networking needs, not just the global backbone). In sum, the combination of seizing technological opportunity, re-designing processes to favor joint warfighters, and setting out coherent governance should allow fast and broad progress toward the vision advanced at the top of this chapter.

Current Issues

Keeping in mind this three-part formula for developing responsive networking, a number of current issues can be addressed.

Should current service programs to enhance network integration be supported?
As noted, all the armed services are now investing in integrated networks of their own. It has been suggested that the path to information integration for joint operations must, or should, pass through integration for each separate service. The theory is that by ensuring that these service systems can "talk to each other," the access and collaboration requirements of joint war-fighting will be met. An alternative view is that heavy investment in intra-service integration will detract from progress toward joint information integration. Which of these views is right depends on the answer to a more fundamental question: How deep should joint operational integration be? A better way to ask it is: How deep should military networks *permit* joint operational integration to be?

By and large, the services still see themselves operating mainly within their own domains at the tactical and operational levels of war, as is evident from the operating concepts that inform their various efforts to organize, train, and equip their respective forces. Cross-service collaboration is seen as exceptional, pre-planned, and to be coordinated by senior joint force commanders (typically, "component commanders," which in fact are extensions of one or another service). Fundamentally, the services do not view joint integration as the correct general model of operations on which to base networking. Consequently, joint connectivity is not a matter of self-interest for the services but instead must be pressed upon them.

The problem is that such a constrained view of operational jointness is self-fulfilling, in that deeper integration is harder to achieve without networks designed to permit and foster it. It does not sufficiently anticipate the *possibilities* for integration and the associated improvement in performance by U.S. forces against all sorts of foes and challenges. This raises a question about the wisdom of counting on service integration efforts as the path to achievement of the strategic objectives of unobstructed access and unbounded opportunities.

To be clear, each service has legitimate reasons to push toward information integration; after all, most operations, including net-centric operations, are among units or platforms of the same service, certainly at the tactical level. Theoretically, if each of the service networks is built to the standards of the established military-wide architecture, the cause of joint integration will be advanced, even if not fully achieved. In reality, however, there are costs associated with ensuring that service networks permit cross-service access and collaboration, and the services must make trade-offs between these cross-service benefits and investments in service weapons and platforms, as well as the capabilities of their own information systems. Is it reasonable to expect the Air Force to make the judgment that it is more important to ensure that Navy aircraft have access to Air Force sensors than it is to have enough or better Air Force aircraft? To the extent that the services believe joint integration will be relatively shallow, they will be disinclined to pay the price, in "hard" capabilities, for information systems that further what may seem distant and unconvincing goals of access and collaboration unobstructed by service boundaries. And they will be ambivalent about connectivity standards.

Consequently, to count on service-led networking investments efforts as the path toward the deep integration vision we have set forth is to ignore their natural tendencies and to rely on imposed yet often ignored standards. Far better to proceed in a way that gathers momentum by following the logic of joint integration, letting users determine needs, and fostering connectivity through self-interest. The pursuit of joint information integration should be a direct one, not via the side-streets of service integration. This is not to say that current service-managed network investments should be cancelled and the goal of intra-service integration discarded. However, the governance troika mentioned above needs to assess the relative importance of intra-service versus inter-service integration and allocate resources for investment accordingly.

How can standards compliance be improved?

The question of standards has come up a number of times already. As Chapter 2 indicates, DOD has tried to use standards to ensure connectivity of networks. In the commercial world, standards—technical guidance on how to connect on the several levels of networking—are considered beneficial by users. There is constant jostling among IT competitors for advantage in standards, both *de jure* and *de facto*. The existence of standards is, after all, what makes networking possible across systems supplied by different vendors. Information users demand connectivity, and information system providers know that failure to meet the demand for connectivity will penalize them. Yet they still add features that compromise interoperability.

Standards are as critical for DOD as they are for any civilian organization, yet harder to achieve because DOD has no dominant provider—nor should it—which is always an option for civilian organizations. The problem at DOD is that there is not a sufficiently strong constituency favoring joint connectivity to counter indifference. As a result, standards are seen not as a compelling virtue but as a costly burden (to the services) or as a time-consuming impediment (to the COCOMs). Waivers to DOD standards are commonly sought and granted on grounds of operational exigency. To the extent standards are relaxed in order to satisfy users, the results do not necessarily promote military-wide connectivity and joint operational integration. DOD must find ways whereby connectivity can be assured, urgent user needs can be satisfied, and standards are embraced rather than imposed.

Important pockets within the services cling to higher priorities than joint integration when it comes to information systems and networks investments, making standards enforcement necessary. In theory, that necessity should diminish as it becomes clear that units that cannot connect cannot operate effectively in a joint force. One of the phenomena of networks, generally speaking, is that prospective users will pay a higher price to join a network as it increases in scale and importance.[39] The deeper the level of operational integration and the stronger the role of the joint community in both setting and fulfilling requirements, the greater the penalty will be for services whose units do not have systems that permit sharing and collaboration. At some point, self-interest in connectivity will prevail: fewer exceptions will be sought; the need to impose and enforce will fade; and connectivity will flourish. When it does, there is still the need to promulgate standards so that this self-interest can be pursued.

Technology should also help move DOD beyond playing "Big Brother" in standards review and enforcement. With the technologies described in Chapter 3, cross-service access and warfighter-to-warfighter collaboration will be possible even in a heterogeneous environment. Connectivity protocols will be aimed more at directory access and less at network interoperability. As a general principle, standards should be tight at levels that ensure user access but not where user creativity, diversity and flexibility are important.

The issue of COCOM adherence to connectivity standards is somewhat different than that of service adherence. The major role for JFCOM prescribed above should remedy the problem of individual COCOMs demanding systems to meet immediate needs without regard to military-wide standards. However, this will only work if the requirements-setting, resource-allocation, and acquisition process are altered to permit speedier response to COCOM demands. A streamlined acquisition process for network systems, with JFCOM as the customer-in-chief, should make it easier to meet immediate user (COCOM) needs without sacrificing military-wide connectivity goals.

It is far too limiting to think of standards as constraints that users must accept at the expense of other goals. The relationship between standards and users is central. Users are

[39] Brian Arthur, an economist, used this observation to explain why investments in networks yield increasing rather than diminishing returns.

both the beneficiary and guiding beacon of standards. Standards give users information integration and permit operational integration, the strategic pay-off of networking. In turn, user satisfaction is the test of standards. In this spirit, a couple of measures would advance the process and results:

- The CIO and/or JFCOM should organize a Users Group to develop a DOD-wide profile for standards development.
- Information integration (i.e., data interoperability) for new systems should be subject to a Joint Test Bed based on operational requirements.

In sum, the technology, process, and governance measures we favor should make standards less contentious without sacrificing connectivity. This could be taken a step further by engaging joint users in guiding and testing standards.

What should be done about legacy systems?
The advent of user-pull technology and service makes legacy systems more widely accessible. Subject to further analysis, it may be that investment in enabling selected older systems to support access and collaboration is an important part of network integration strategy.

The cost of legacy systems is largely sunk and thus of no economic significance. The ease of access—and the extent of investment required to permit access—will vary among them. Apart from this, some have better functions and features than others. It seems likely that investment in those that do not require much to be accessible and have valued features and functions may be a better way to spend the next dollar than acquiring some new system. Put differently, the case for investment in new systems should be based more on features, functionality and other qualities and less on network interoperability, assuming new user-pull technologies realize their promise.

The legacy problem may be less serious than once thought—i.e., that the cost-effectiveness of legacy systems may be looking better, thanks to the declining cost of making them more effective. Case-by-case analysis is more important than sweeping policy. But it is essential that the objectives of unobstructed access and unbounded collaboration be used as the business-case standards for both old and new systems. The number of legacy systems retired is not a good measure of progress toward integration. On the whole, the bias should be toward using legacy systems.

What are the roles for defense systems integrators and IT firms?
Defense systems integrators once had an indispensable role in creating IT solutions to military needs. When systems were based on proprietary (closed) architectures, integrators had to write the software to make them work together. Moreover, instead of trying to sell this or that computer or telecommunications gear, they were driven by the operational missions and requirements of the customer, which they made a point of understanding. More recently, open systems reduce the need for heavy integration work, and smarter users are more able to tailor technology to their needs—sort of like buying a Dell computer—without having to rely heavily on an integrator.

Meanwhile, firms that excel in the creation and application of information technology largely shun the market for major "defense systems" in favor of the easier, larger, and more lucrative commercial markets.[40] They lack the business model, market knowledge (very important in defense, of course), account access, and acquisition-process savvy that the defense systems integrators have. Consequently, although the average content—the portion of new military systems—required of the integrators may have shrunk, their position is increasingly that of a "principal agent" (in economic theory) for defense customers—prime contractors whose main function is to manage and marry customers with IT sub-contractors. In turn, customers and IT firms find it easier to work through the integrators than not.

It is not clear that this pattern is advantageous for either the warfighter or the taxpayer. The benefits of direct involvement by IT firms in meeting military network needs could be significant:

- The distance between the military user and the source of IT could be shortened.
- Costs could be reduced.
- Faster response could be expected.
- Greater exploitation of successful commercial solutions could be possible.
- Greater competition could be introduced into DOD information/network markets.

This does not exclude a role for systems integrators (or principal agents). Their customer/mission knowledge is valuable and not easily replicated, and the need for true systems integration could be great in particular cases. All the same, the option of working directly with IT firms is increasingly important. Of course, this is far more likely to happen if the acquisition process for C4 is made more attractive, as already suggested.

How can user-pull be reconciled with information assurance and security?
This paper need not belabor the importance of security, and the ways of providing security are beyond its scope. However, it is only fair to note how difficult it will be to improve and assure security when trying to maximize user-pull and collaboration. The cornerstone of security—before and during the age of networks—is that "need to know" certain information should not be decided by the party with that need, but instead by the steward of the information or a third party. The cornerstone of user-pull is the primacy of the user's own judgment of need, not only to warrant access but to drive solutions, protocols, and architecture. Conversely, unobstructed access, information integration, and deep, fluid operational integration could be impeded by accepted security strategies.

We cannot solve this problem in this paper. However, we can say that it is unlikely to be solved without the most intimate collaboration between the defense establishment and the leading firms and minds of the IT world. DOD should find a way to engage none other than the wizards of the Internet, who have developed methods and engines to give users instant access to untold stores of information, in the challenge of reconciling user supremacy with the information security on which national security depends.

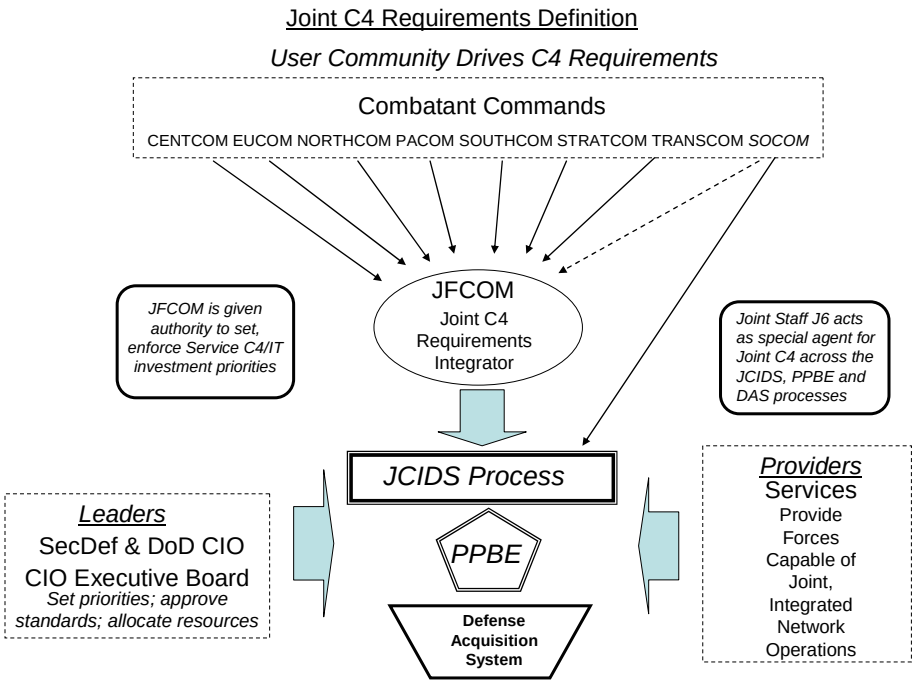
[40] Some major defense-systems players of the Cold War—IBM, GE, Unisys, and AT&T, for example—shrank or shed those businesses as the information revolution gathered steam in the 1980s.

Conclusions and Specific Recommendations

We have made some rather sweeping suggestions based on a broad survey of what is happening both inside and outside of DOD in regard to responding to information user needs. The need for a bold approach to joint C4 lies in the importance of the opportunity the defense establishment has at this moment to push its exploitation of information "to the next level" and beyond. We observe that the major information challenge facing DOD today—giving end-users, from top to bottom, greater access and ability to collaborate—is precisely the main challenge being addressed in the larger world of IT. This is no coincidence: with the growth of network infrastructure, usage, services, and expectations in both military and civilian sectors, it stands to reason that users now want huge pay-offs in ways that will help them—again, access and collaboration. In theory, this is fortuitous. Like other sectors—health, finance, travel—defense needs to seize this opportunity quickly and firmly. In practice, however, defense does not have the mechanisms to seize the opportunity quickly and firmly. DOD still, for the most part, tries to exploit information technology the same way it designs and builds ships, tanks and missiles. As is evident from the demands for standards waivers, fast-track acquisition, and other exceptions, established processes cannot connect DOD's strategic need for information integration with IT's strategic offer of information integration.

Accordingly—based on a review that is admittedly broader than it is deep—we have suggested the creation of a new regime of governance, requirements-setting, resource-allocation, acquisition, alignment of authority, and other steps to empower users. This regime would focus on C4 needs that flow from the vision of deeply integrated and highly fluid operations and be designed to maximize DOD exploitation of the gathering wave of user-reach technology and ideas. While this regime would differ sharply from DOD's standard business processes, it would conform to core tenets of public spending. It would also be limited to those missions, solutions and systems that bear on *joint* information integration, though more and more C4-IT investment could be drawn in as integration becomes deeper.

This regime for responding to joint C4 information needs is depicted in the following two figures. The first one highlights the centrality of JFCOM in integrating user (i.e., joint warfighter) needs, obtaining the resources to meet them, and serving as the principal customer in the acquisition process. SECDEF's main responsibilities are to see to it that joint C4 is treated as a national strategic priority, that DOD business processes are coupled to the operational-information needs of joint C4 users—by giving them economic power—and that funding is adequate. The CIO should ensure that both SECDEF's strategic goals and JFCOM's operational needs are addressed in practice. The Joint Staff (J-6) should serve as the agent of JFCOM in DOD's requirements-setting and resource-allocation processes. Any of the several armed services may be called upon by JFCOM to execute acquisition decisions for joint C4, in addition to meeting their own service-unique needs. The second figure shows in more detail the roles of the principal actors—leaders, users, providers, and supporters—at various stages in the process.



Needed: A Separate Top-Down, User-In Process to Provide Joint C4/IT

Goal: Cut process times by 50% or more	C4/IT Requirements (Abbreviated JCIDS)	C4/IT Funding (Abbreviated PPBE)	C4/IT Acquisition (Expedited DAS)	Net Centric Operations & Warfare (NCOW)
SECDEF	Set NCOW goals and measure results	Approve Joint C4/IT funding level and budgets	Set up separate, simplified C4/IT AS; Approval authority	Oversee Joint Ops and Warfighting
DoD CIO	Set architecture and enforce standards	Set Joint C4 priorities and approve Service C4 budgets with JFCOM	Oversee a new, faster C4/IT Acquisition System (C4/IT AS)	Highest operational support; Joint C4 problem solver
JFCOM	Integrate COCOM Inputs; set Joint C4 requirements	Earmarks funds for integrated, prioritized COCOM Requirements	With SOCOM, *the* Joint C4 Operational Customer(s)	Joint C4/IT lessons Learned
COCOMs	Input operational C4 requirements	Support Integrated Joint C4/IT Priorities	Support Integrated Joint C4/IT Priorities	Operational Joint C4 Users
STRATCOM	Input global network requirements	Develop GIG budget and funding priorities with DoD CIO, DISA	*the* Joint C4 Strategic Customer	Operate and Defend GIG (JTF-GNO), Conduct Strategic IO
Services	Integrate JFCOM C4/IT requirements into Service programs, forces	Fence off funding for Joint C4/IT identified by JFCOM as approved by DoD CIO	Procure Joint C4 prioritized, earmarked by JFCOM	Provide Joint Network Capable forces to COCOMs
JCS-J6	Action agent for Joint C4/IT requirements on behalf of JFCOM	Action agent for Joint C4/IT funding on behalf of JFCOM	Action agent for Joint C4/IT acquisition on behalf of JFCOM	Direct Joint C4 operational support to COCOMs
DISA	Provide Joint Technical expertise and support	Technical expertise and common support	Technical expertise and common support	Direct technical support to COCOMs

* DoD C4/IT Leaders * C4/IT Users * C4/IT Providers * C4/IT Supporters

DOD often finds it useful to experiment with new ideas, especially those that involve major departures from existing practices or structures. Such experimentation might be indicated in this case, for instance:

- JFCOM could be given responsibility, authority and resources to invest in joint C4 on a limited basis (as recommended by a separate study).[41]
- JFCOM and one or more COCOMs could experiment with "user reach" techniques to access information and collaborate across networks and to shape user-in information solutions.
- One or more service network-integration program could be subject to the test of *deep (joint) integration* presented here, using joint warfighters to uncover limits on access and collaboration.

While recognizing the value of such experiments, we urge that DOD's civilian and uniformed leadership understand and share a holistic view of the challenge of strengthening governance, reforming business processes, and exploiting user-reach technology strategically. A few experiments and incremental changes will not ensure that DOD will catch this wave. Only a new regime, at least to govern joint C4, will.

Along with such a new regime, we offer a number of observations about issues:

- A strategy of creating intra-service integration as the route to inter-service integration is questionable. Service investments in C4 generally and C4 integration in particular should stand on their own merits and not as a contribution to information jointness.
- With improved user-access technologies, stovepipe legacy systems may be more serviceable than previously thought.
- The need to impose and enforce tight standards should be superseded by a growing constituency for connectivity, which should be given more power in setting and meeting requirements.
- Every effort should be made to attract IT firms into major and direct business with DOD.
- It will take the creative genius of the IT industry to reconcile the need for security with the tenets of user-need. In the end, the information security that comes from restricting access will have to be weighed carefully against the national security that comes from deep integration.

Acknowledging the need for more thorough analysis and debate before such suggestions are accepted, we recommend such analysis and debate as a matter of urgent national security priority.

[41] Franklin Kramer and Stuart Starr, "*Actions to Enhance the Use of commercial Information Technology in DOD Systems.*" (Washington, DC: Center for Technology and National Security Policy, 2005).